EnGenius®

User Manual

ESR9855G

Wireless 300N Gigabit Gaming Router

Gigabit & StreamEngine Support

EnGenius®

Table of Contents

1. INTRODUCTION 7

1.1. FEATURES & BENEFITS 7
1.2. PACKAGE CONTENTS 9
1.3. SAFETY GUIDELINES 9
1.4. WIRELESS SOHO ROUTER DESCRIPTION 10
1.5. SYSTEM REQUIREMENTS 12
1.6. APPLICATIONS 12
1.7. NETWORK CONFIGURATION 14
a) Ad-hoc (peer-to-peer) Mode 14
b) Infrastructure Mode 15

2. UNDERSTANDING THE HARDWARE 16

2.1. HARDWARE INSTALLATION 16
2.2. IP ADDRESS CONFIGURATION 17

3. LOGIN 19

4. INTERNET SETTINGS 20

4.1. INTERNET CONNECTION TYPE 21
4.1.1. DHCP Connection (Dynamic IP Address) 22
4.1.2. PPPoE (Point-to-Point Protocol over Ethernet) 23
4.1.3. PPTP (Point-to-Point Tunneling Protocol) 25
4.1.4. Static IP Address Configuration 27
4.2. OTHER INTERNET SETTINGS 28
4.2.1. RIP (Routing Information Protocol) 28
4.2.2. DNS Settings 29
4.2.3. MTU Settings 29
4.2.4. WAN Ping 30
4.2.5. Multicast Streams 30
4.2.6. MAC Cloning 31

5. WIRELESS SETUP WIZARD 32

5.1. WIRELESS NETWORK WIZARD SETUP 32
5.1.1. Automatic Network Setup 33
5.1.2. Manual Network Setup 34

EnGenius®

5.1.2.1. Wireless Security Level: BEST (WPA2) 37
5.1.2.2. Wireless Security Level: BETTER (WPA) 38
5.1.2.3. Wireless Security Level: GOOD (WEP 64/128-bit) 40
5.1.2.4. Wireless Security Level: None (Security Disabled) 42

6. MANUAL WEB CONFIGURATION 43

6.1. LOGGING IN 43
6.2. BASIC 44
6.2.1. Internet Settings 44
6.2.2. Wizard Wireless 44
6.2.3. Network Settings 45
6.2.3.1. Bridge Mode 45
6.2.3.2. Router Mode 46
6.2.4. Wireless Settings 54
6.2.4.1. Wireless Security Mode 56
6.2.4.2. WEP (Wired Equivalent Privacy) 57
6.2.4.3. WPA Personal (Wi-Fi Protected Access) 58
6.2.4.4. WPA Enterprise (Wi-Fi Protected Access & 802.1x) 59
6.3. ADVANCED 61
6.3.1. Advanced Wireless 62
6.3.2. Virtual Server 64
6.3.3. Special Applications 66
6.3.4. Port Forwarding 67
6.3.5. StreamEngine 69
6.3.6. Routing 73
6.3.7. Access Control 74
6.3.8. Web Filter 78
6.3.9. MAC Address Filter 79
6.3.10. Firewall 80
6.3.11. Inbound Filter 84
6.3.12. WISH 85
6.3.13. Wi-Fi Protected Setup 87
6.3.14. Advanced Network (UPNP, WAN Ping…) 88
6.4. TOOLS 90
6.4.1. Time Zone Setting 91
6.4.2. System 92
6.4.2.1. Save To Local Hard Drive 93
6.4.2.2. Load From Local Hard Drive 93

EnGenius®

6.4.2.3. Restore To Factory Default 94
6.4.2.4. Reboot the device 95
6.4.3. Firmware Upgrade 96
6.4.4. System Logs 97
6.4.5. Dynamic DNS 98
6.4.6. System Check 99
6.4.7. Schedules 100
6.5. STATUS 101
6.5.1. Wireless Status 102
6.5.2. Logs Status 103
6.5.3. Statistics 104
6.5.4. WISH Session Status 105
6.5.5. Routing 107
6.5.6. Internet Session Status 108
6.5.7. Firewall 110

APPENDIX A – GLOSSARY 111

8 112
A 112
B 113
C 114
D 114
E 116
F 116
G 117
H 117
I 118
J 119
K 119
L 120
M 120
N 121
O 122
P 122
Q 123
R 123
S 124
T 125
U 125
V 126

W 126
X 127
Y 127

APPENDIX C – FCC INTERFERENCE STATEMENT 129

1. Introduction

The Wireless-N Gigabit Router is a 802.11n compliant device that delivers up to 6x faster speeds than 802.11g while staying backward compatible with 802.11g and 802.11b devices.

It is not only a Wireless Access Point, which lets you connect to the network without wires. There's also a built-in 4-port full-duplex 10/100/1000 Gigabit Switch to connect your wired-Ethernet devices together. The Router function ties it all together and lets your whole network share a high-speed cable or DSL Internet connection.

The Access Point built into the Router uses advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple steams of data in a single wireless channel. The robust signal travels farther, maintaining wireless connections up to 3 times farther than standard 802.11g, eliminates dead spots and extends network range.

To protect the data and privacy, the Router can encode all wireless transmissions with 64/128-bit encryption. It can serve as your network's DHCP Server, has a powerful SPI firewall to protect your PCs against intruders and most known Internet attacks, and supports VPN pass-through. The router also provide easy configuration with the web browser-based configuration utility.

The incredible speed and QoS function of 802.11n Gigabit Router is ideal for media-centric applications like streaming video, gaming, and VoIP telephony. It is designed to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

This chapter describes the features & benefits, package contents, applications, and network configuration.

1.1. Features & Benefits

Features	Benefits
High Speed Data Rate Up to 300Mbps	**Capable of handling heavy data payloads such as MPEG video streaming**
IEEE 802.11n Compliant and backward compatible with 802.11b/g	**Fully interoperable with IEEE 802.11b/g/n devices**
Four built-in 10/100/1000Mbps Gigabit Switch Ports (Auto-Crossover)	**Scalability, able to extend your network**

Supports DNS/ DDNS	**Lets users assign a fixed host and domain name to a dynamic Internet IP address.**
Supports NAT (Network Address Translation)/NAPT	**Shares single Internet account and provides a type of firewall by hiding internal IP addresses for keeping hacker out**
Hide SSID	**Avoids unallowable users sharing bandwidth, increases efficiency of the network**
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	**Avoids the attacks of Hackers or Viruses from Internet**
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-thru mechanisms	**Provide mutual authentication (Client and dynamic encryption keys to enhance security**
WDS (Wireless Distribution System)	**Make wireless AP and Bridge mode simultaneously as a wireless repeater**
Universal Plug and Play (UPnP™)	**Works with most Internet gaming and instant messaging applications for automatic Internet access**
Filter Scheduling	**The filter can be scheduled by days, hours or minutes for easy management**
Real time alert	**The detection of a list for Hacker log-in information**
Web configuration	**Helps administrators to remotely configure or manage the Router via Telnet/Web-browser**

1.2. Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- Wireless Gaming Router x 1
- Power Adapter x 1
- 3dBi 2.4GHz Dipole Antennas x 2
- CD-ROM with User Manual x 1
- Quick Guide x 1

1.3. Safety Guidelines

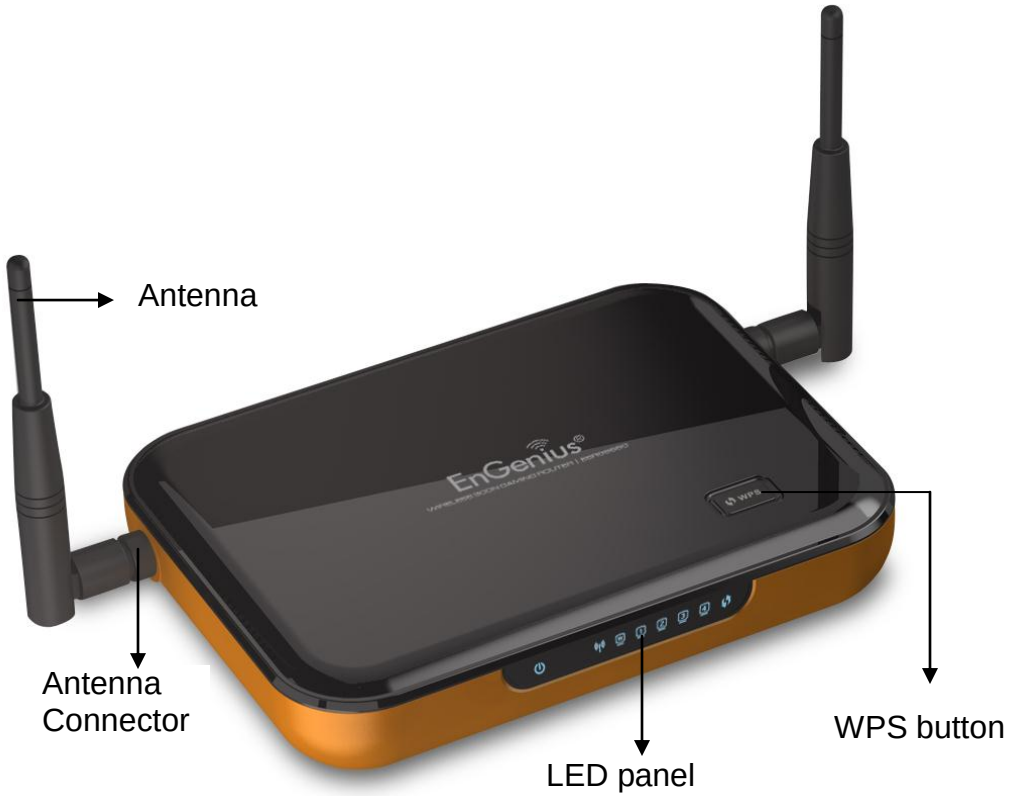
In order to reduce the risk of fire, electric shock and injury, please adhere to the following safety guidelines.

- Carefully follow the instructions in the User Manual and also follow all instruction labels on this device.
- Except for the power adapter supplied, this device should not be connected to any other adapters except the supplied one.
- Do not spill liquid of any kind on this device.
- Do not place the device on an unstable stand or table. .
- Do not expose this unit to direct sunlight.
- Do not place any hot devices close to the device, as they may degrade or cause damage to the unit.
- Do not place any heavy objects on top of the device.
- Do not use liquid cleaners or aerosol cleaners. Use a soft dry cloth for cleaning.

1.4. Wireless SOHO Router Description

Rear Panel

Front Panel



Parts	Description
LAN Ports (1 – 4)	Use an Ethernet cable to connect each port to a computer on your Local Area Network (LAN).
WAN Port	Use an Ethernet cable to connect this port to your WAN router.
Antenna Connector	Interface for the antennas.
LAN LED	This LED will light up once an Ethernet cable is connected to one of the LAN ports.
WAN LED	This LED will light up once an Ethernet cable is connected to WAN (Internet) port.
WLAN LED	This LED will light up once the RF (wireless LAN) feature is enabled
Power LED	This LED will light up once the power cable is connected to the DC connector.
WPS button	1- 5 seconds: activates WPS 6-10 seconds: reboot 11~ seconds: reset to default
Power Switch	Turn on or off the device

1.5. System Requirements

The following are the minimum system requirements in order to configure the device.

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser

1.6. Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) The ability to access real-time information

Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) Frequently changed environments

Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) Small Office and Home Office (SOHO) networks

SOHO users need a cost-effective, easy and quick installation of a small network.

f) Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

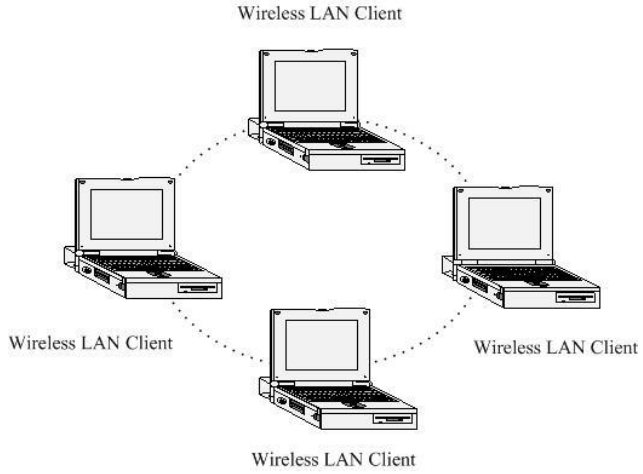
1.7. Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
b) Infrastructure for enterprise LANs.

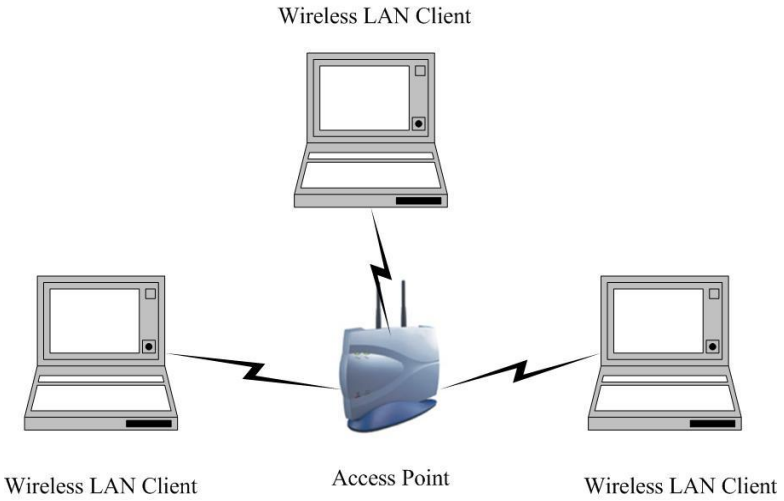
a) Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.

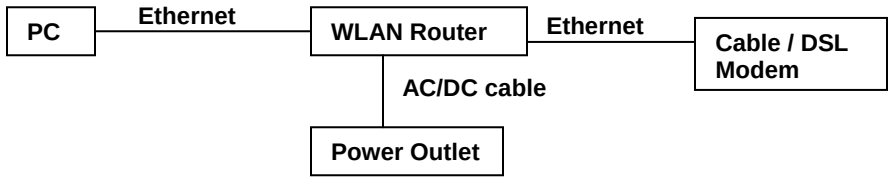


2. Understanding the Hardware

2.1. Hardware Installation

1. Place the device in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the LAN port of the device and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to WAN port of the device and the other end into you cable/DSL modem (Internet)
4. Insert the DC-inlet of the power adapter into the port labeled “POWER” and the other end into the power socket on the wall.

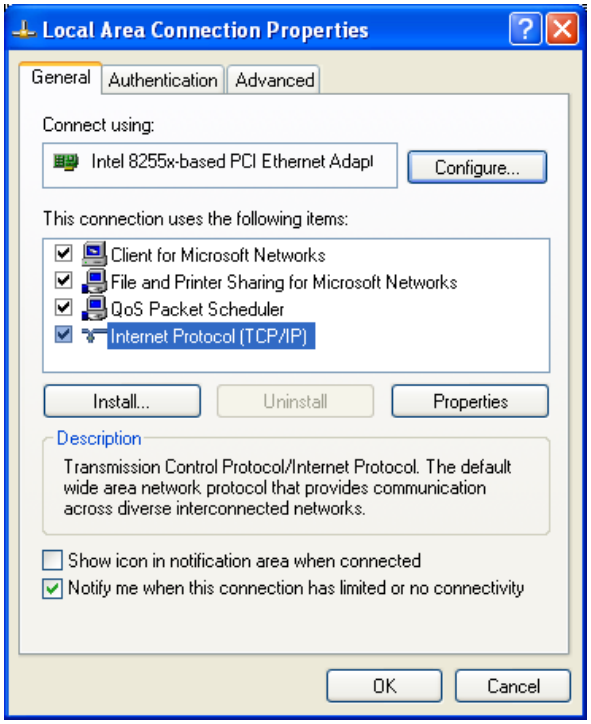
This diagram depicts the hardware configuration



2.2. IP Address Configuration

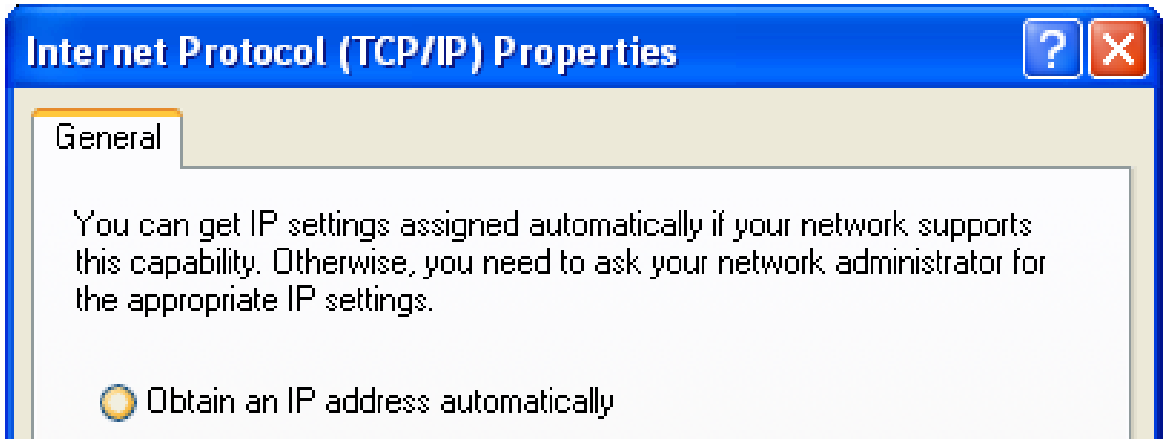
This device can be configured as a Bridge/Router or Access Point. The default IP address of the device is **192.168.1.1** In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



EnGenius®

2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Laptop.

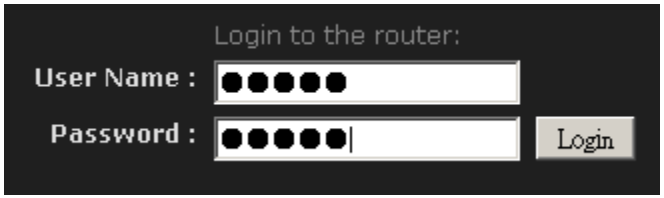


Select **Obtain an IP address automatically** radio button.

3. Click on the **OK** button to close this window, and once again to close LAN properties window.

3. Login

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the URL bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to previous chapter in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page. Enter **admin** for both User Name and Password. Click on [**Login**] to enter the administration page..

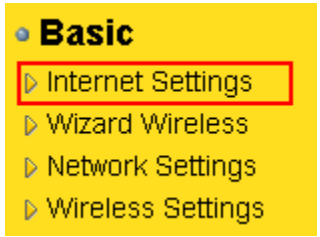


4. Internet Settings

This device offers a quick and simple configuration through the wizard. This chapter describes how to use the wizard to configure the WAN, LAN, and wireless settings. Please refer to Chapter 6 in order to configure the more advanced features of the device.

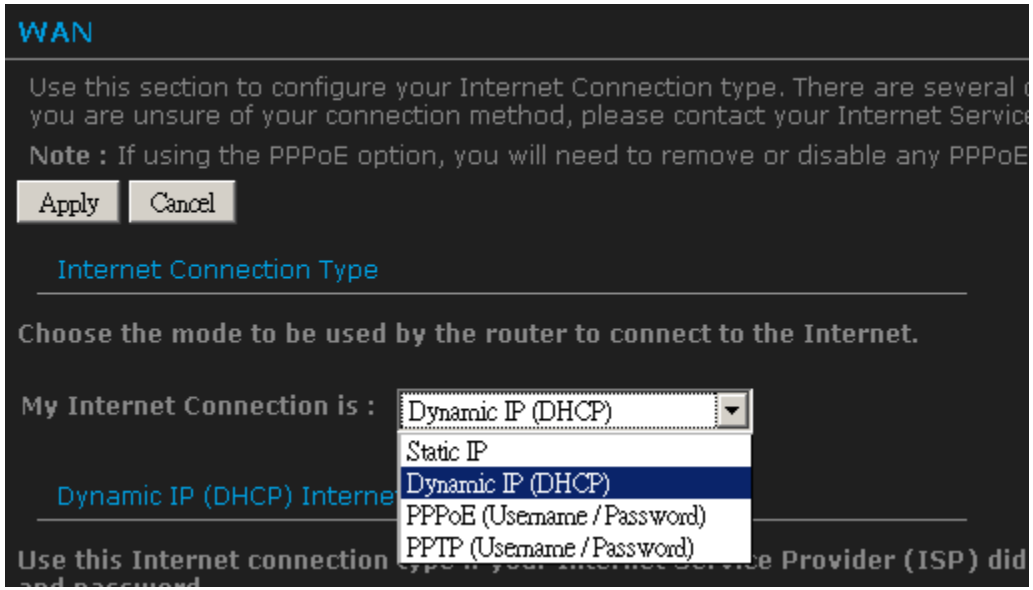
IMPORTANT NOTICE

Internet Settings Page contains various settings related to WAN / Internet service. Usually, you only need to configure **Internet Connection Type** section to connect to the Internet. Unless your ISP specified otherwise, please keep the default settings if you are unsure of the configuration. Please consult your local ISP for your Internet Connection Type and account information.



- The configuration wizard for each connection type is described below.
- Click on the **Internet Settings** to begin the process.

4.1. Internet Connection Type



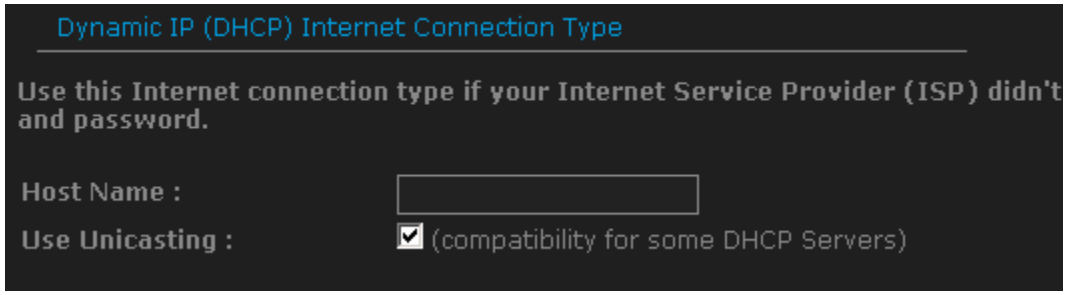
- Select your Internet service WAN type

- This device supports several types of Internet / WAN connections:
  - **DHCP Connection (Dynamic IP address)** – Choose this connection type if your ISP provides you the IP address. Most cable modems use this type of connection.
  - **PPPoE (Poinit-to-Point Protocol over Ethernet)** – Choose this option if your internet connection requires a user name and password. Most DSL modems use this type of connection.
  - **PPTP (Point-to-Point Tunneling Protocol)** – Choose this type of connection if your ISP requires to use PPTP. Your ISP should provide you with a user name and password.
  - **Static IP address** – Choose this option if you have a dedicated IP address.

- Page content will change in accords to the Internet Connection option. Please consult your local ISP for the appropriate choice. The following sections explain the supported Internet type.

4.1.1.DHCP Connection (Dynamic IP Address)

The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

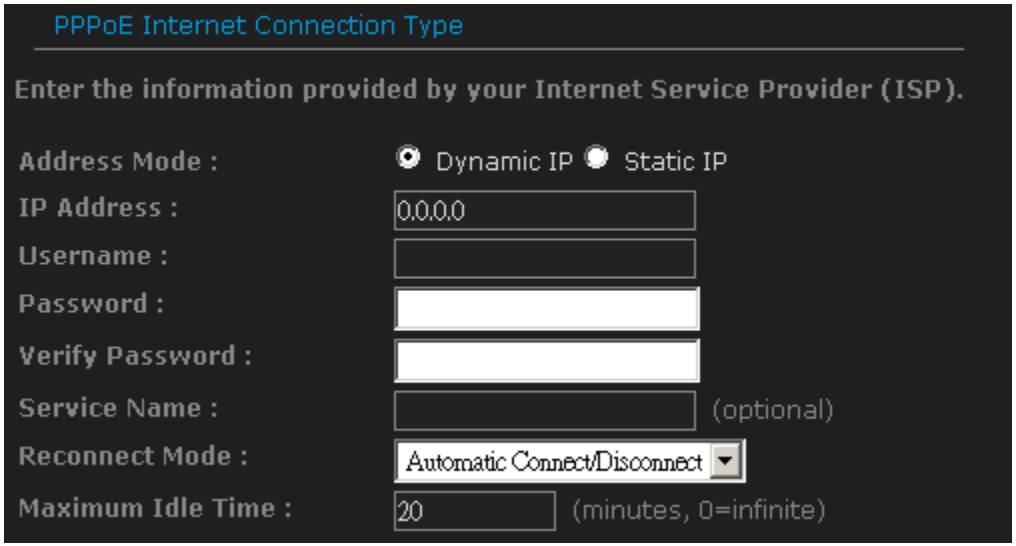


Host Name: this is optional if you need to specify the host name for this router.

Use Unicasting: This option is normally turned off, and should remain off as long as the WAN-side DHCP server correctly provides an IP address to the router. However, if the router cannot obtain an IP address from the DHCP server, the DHCP server may be one that works better with unicast responses. In this case, turn the unicasting option on, and observe whether the router can obtain an IP address. In this mode, the router accepts unicast responses from the DHCP server instead of broadcast responses.

4.1.2. PPPoE (Point-to-Point Protocol over Ethernet)

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.



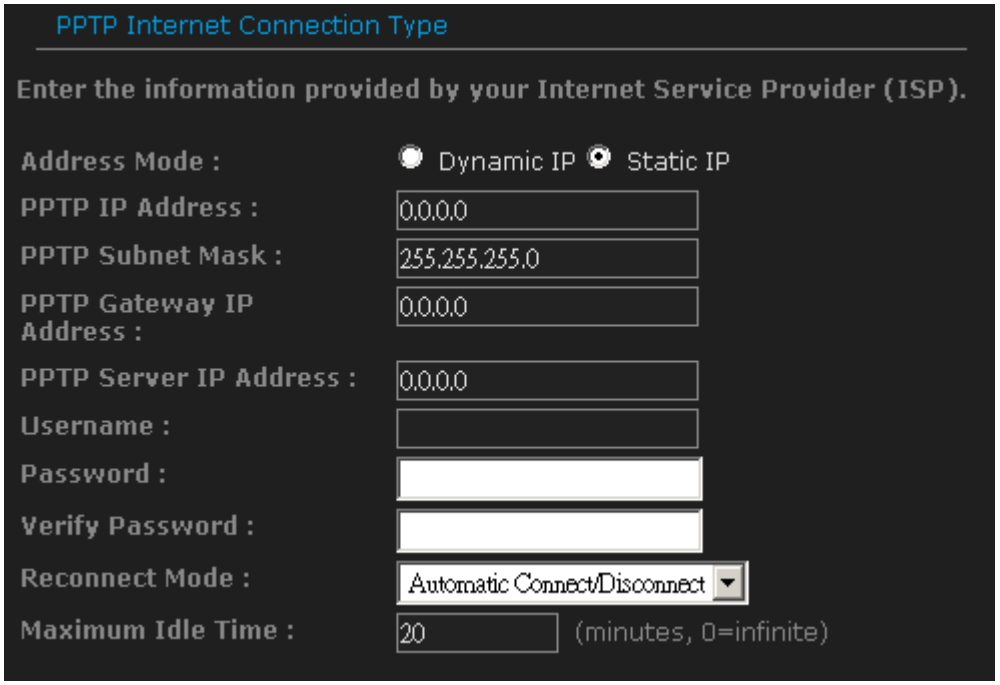
- **Address Mode**: PPPoE can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IIP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **IP Address**: Specify the IP address if the Static IP is selected.
- **User Name**: Specify the username which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Verify Password:** Enter the password again for verification
- **Service Name:** Specify the name of the ISP. This is optional.
- **Reconnect Mode:**
    - Keep Connection: This option provides a continuous connection.

- Automatic Connect: This option provides an automatically connect.
- Manual Connect: This option provides a connection on demand.

- **Maximum Idle Time:** Specify the maximum idle time (disconnect when device is idled over the specified period.

4.1.3. PPTP (Point-to-Point Tunneling Protocol)

- PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a username and password (provided by your ISP) to gain access to the Internet. The supported authentication protocols are PAP and CHAP.

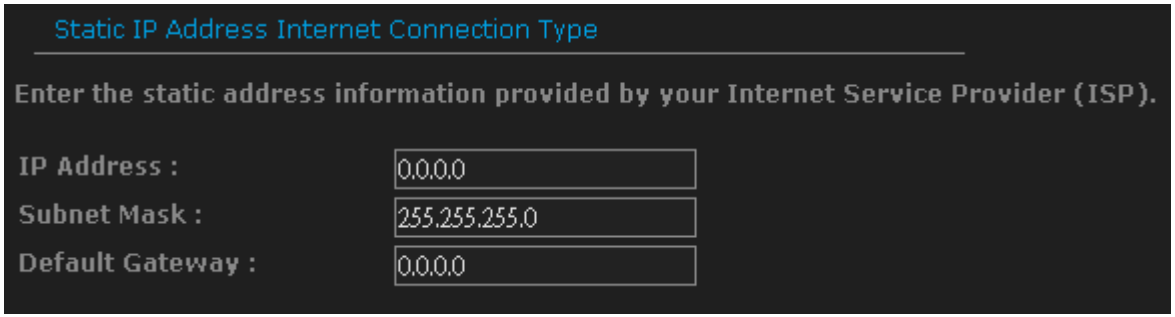


- **Address Mode**: PPTP can be used with a dynamic or static IP address. If you select the **Dynamic IP** radio button, then the IIP address in the next field is not required. However, if you select the **Static IP** radio button, then the IP address in the next field is required.
- **PPTP IP Address**: Specify the IP address
- **PPTP Subnet Mask**: Specify the subnet Mask for the IP address.
- **PPTP Gateway IP Address**: Specify the IP address of the PPTP gateway.

- **PPTP Server IP Address**: If the PPTP Server's IP address is different from the default gateway, then you may specify it here.
- **Usernname**: Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Verify Password:** enter the password again for verification
- **Reconnect Mode:**
    - Keep Connection: This option provides a continuous connection.
    - Automatic Connect: This option provides an automatically connect.
    - Manual Connect: This option provides a connection on demand.
- **Maximum Idle Time:** Specify the maximum idle time (disconnect when device is idled over the specified period.

4.1.4. Static IP Address Configuration

- In this type of connection, your ISP provides you with a dedicated IP address.



- **IP Address:** Specify the IP address for the device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- **Gateway Address:** Specify the IP address of the default gateway, which is assigned by your ISP.

- Usually, Static IP Address needs to specify DNS setting; please configure your DNS setting.

- **Primary / Secondary DNS Address:** Specify the primary and secondary IP address, which is assigned by your ISP.

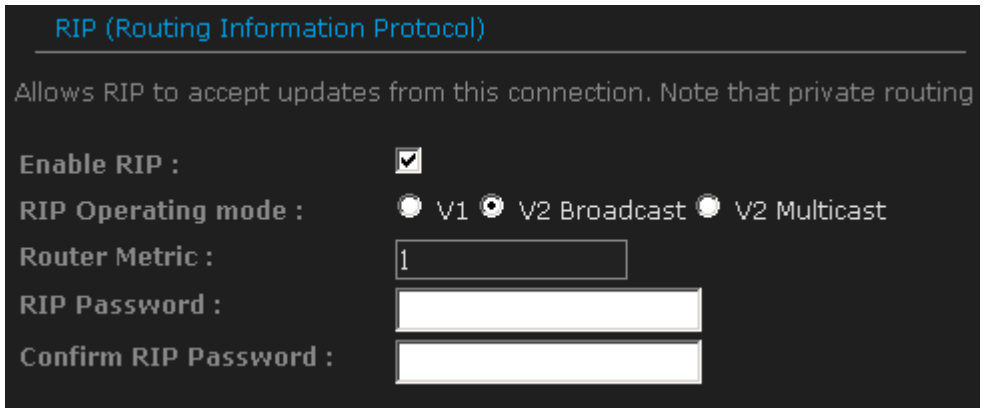
4.2. Other Internet Settings

IMPORTANT NOTICE

Internet Settings Page contains various settings related to WAN / Internet service. Usually, you only need to configure **Internet Connection Type** section to connect to the Internet. Unless your ISP specified otherwise, please keep the default settings if you are unsure of the configuration. Please consult your local ISP for your Internet Connection Type and account information.

4.2.1. RIP (Routing Information Protocol)

This function allows RIP to accept updates from this connection. Note that private routing information is never sent to this connection.



4.2.2.DNS Settings

Most of the ISP does not require user to specify DNS settings. In case where DNS needs to be specified you can change the setting in this section.

4.2.3.MTU Settings

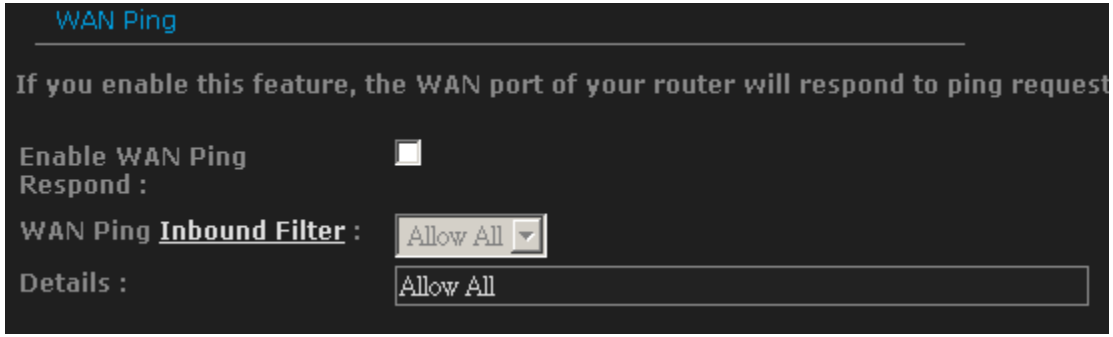
Most of the ISP does not require user to specify MTU settings. In case where MTU needs to be specified. You can change the setting in this section.

- **MTU**: The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

4.2.4.WAN Ping

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Respond: checking the box.



You can specify the Inbound Filter and choose whether to **Allow All** or **Deny All**.

4.2.5.Multicast Streams

Enable Multicast Streams: checking the box if you have multicast streaming service on your local network.

4.2.6.MAC Cloning

MAC Address: specify the MAC address.
Click on **[Clone Your PC's MAC address]** button to enter the MAC address of your PC/laptop automatically.

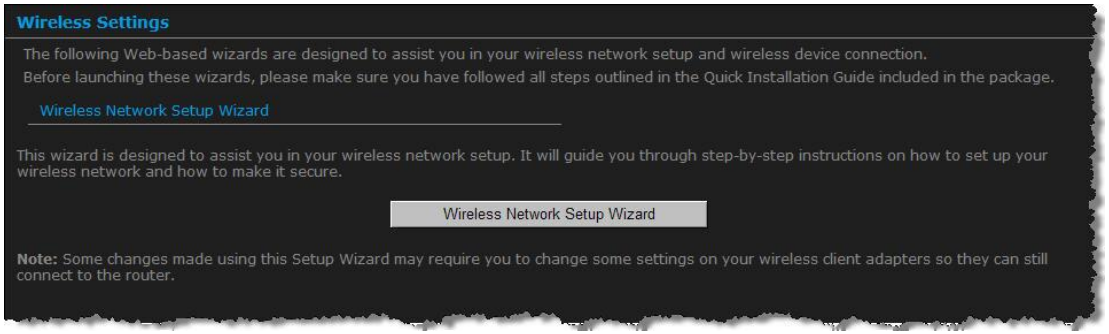
5. Wireless Setup Wizard

This wizard will guide you in the configuration of the wireless network settings such as the SSID and security (WEP/WPA).

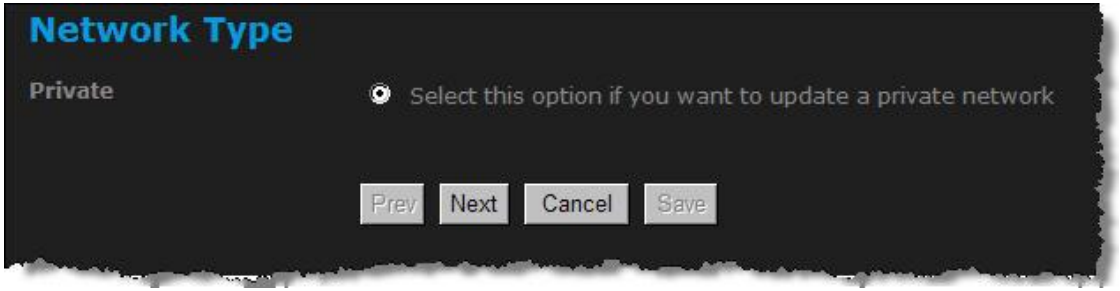
.Please refer to Chapter 6 in order to configure more advanced features of the device

5.1. Wireless Network Wizard Setup

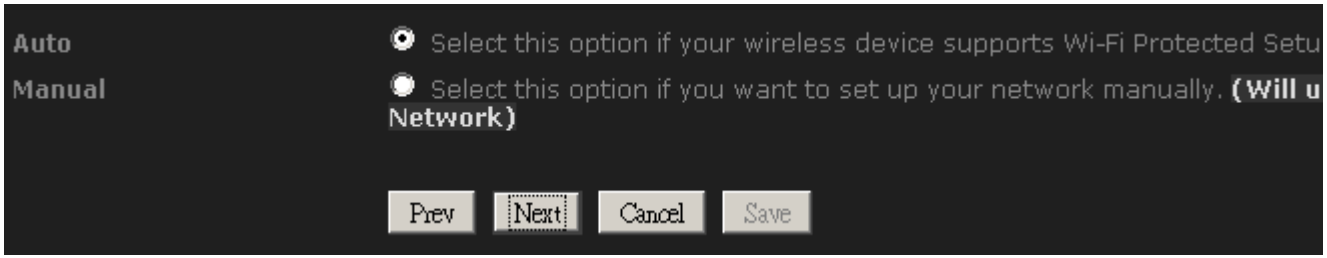
- Click on the **Wizard Wireless** link under the **Basic** menu, and then click on the **Wireless Network Setup Wizard** button.



EnGenius®

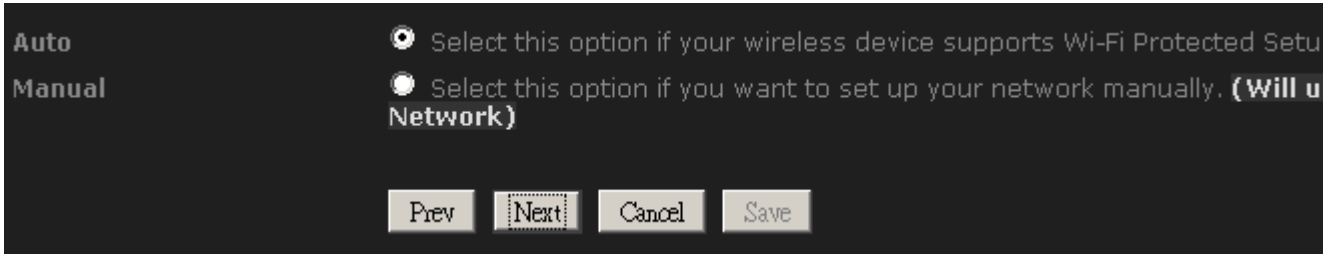


- The wizard will inform you that there are two options: auto and manual.



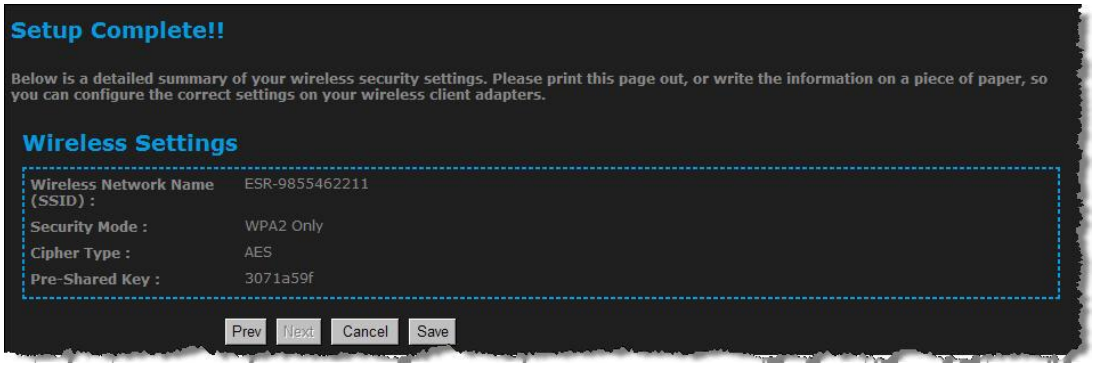
5.1.1. Automatic Network Setup

- If you select the **Auto** option, then the device will automatically configure the SSID and security mode.



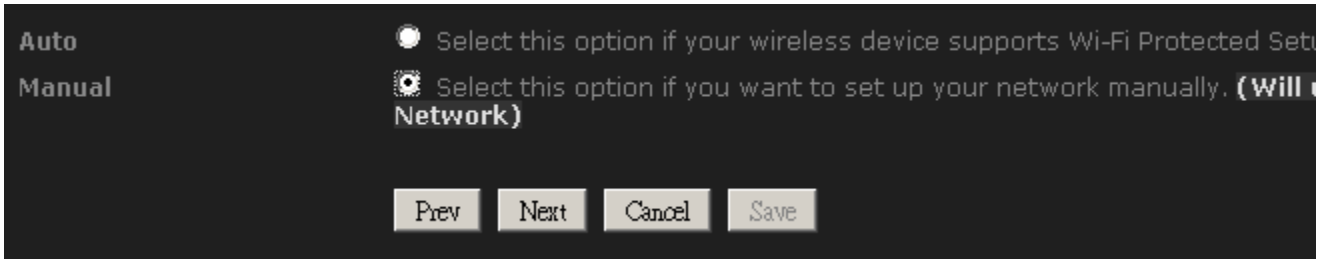
- Click on the **Next** button to continue.

- The wizard has automatically configured the SSID and security mode for the device. Click on the **Save** button to complete the setup.

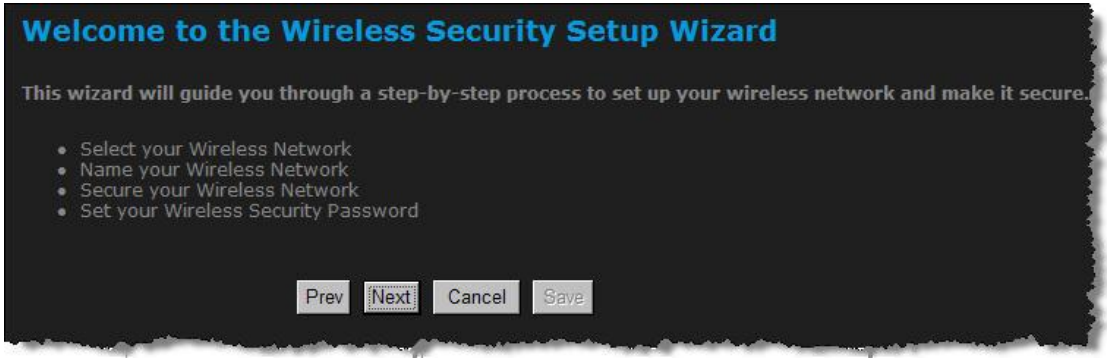


5.1.2. Manual Network Setup

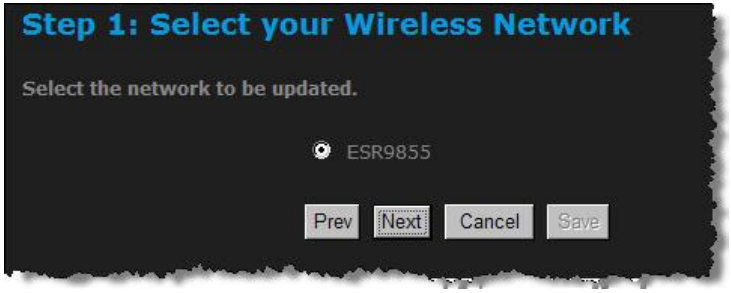
- If you select the **Manual** option, then you will be required to specify the SSID and select the appropriate network security.
- Click on the **Next** button to continue.



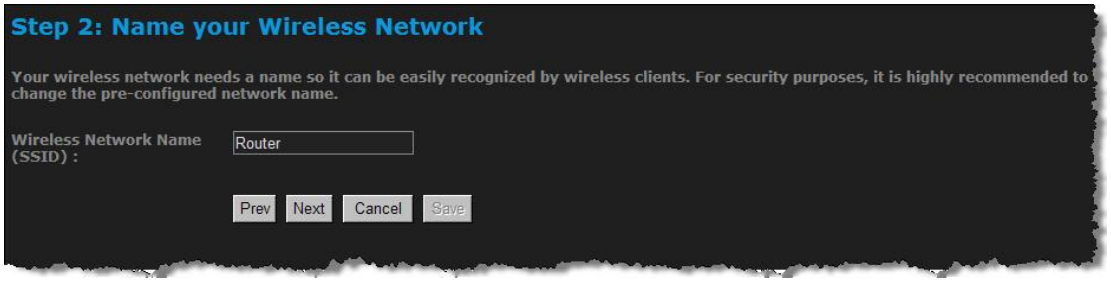
- The wireless wizard will inform you that there are three major steps in the process.
  - Name your wireless network
  - Secure your wireless network
  - Set your wireless security password



- Click on the **Next** button to continue.



- Specify the Wireless Network Name (SSID) for the device. The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. Click on the **Next** button to continue.



EnGenius®

- This step requires that you configure the security features based on your needs. The following options are available.
  - **BEST** – Select this option if your wireless adapters support WPA2
  - **BETTER** – Select this option if your wireless adapters support WPA
  - **GOOD** – Select this option if your wireless adapters do not support WPA, but support WEP instead
  - **None**: Select this option if you do not want to activate any security features.

- In order to protect your network from hackers and unauthorized users, it is highly recommended to secure the network using encryption and authentication. Select a level of security and then click on the **Next** button to continue.
- If you do not want to setup security, then select the **NONE** radio button.

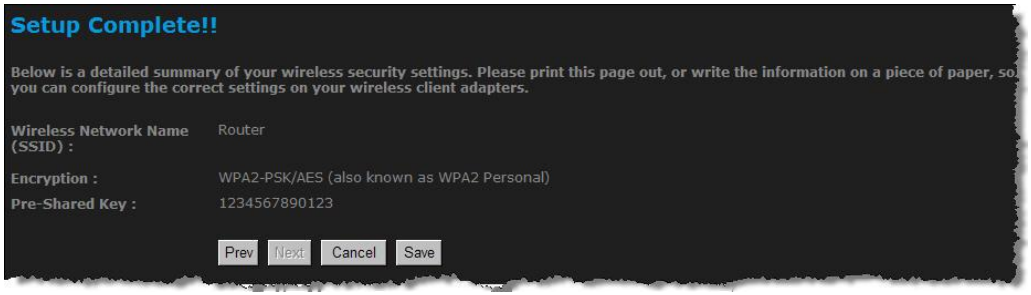
EnGenius®

5.1.2.1. Wireless Security Level: BEST (WPA2)

- Select the **BEST** radio button which supports WPA2 encryption. Then click on the **Next** button.

- Enter a security password between 2 and 20 characters then click on the **Next** button.

- The setup is complete. Click on the **Save** button and then reboot the device.



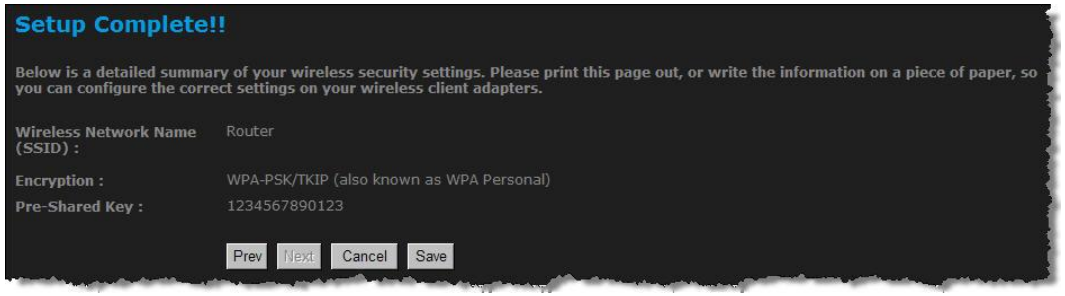
5.1.2.2. Wireless Security Level: BETTER (WPA)

- Select the **BETTER** radio button which supports WPA encryption. Then click on the **Next** button.

- Enter a security password between 2 and 20 characters then click on the **Next** button.

EnGenius®

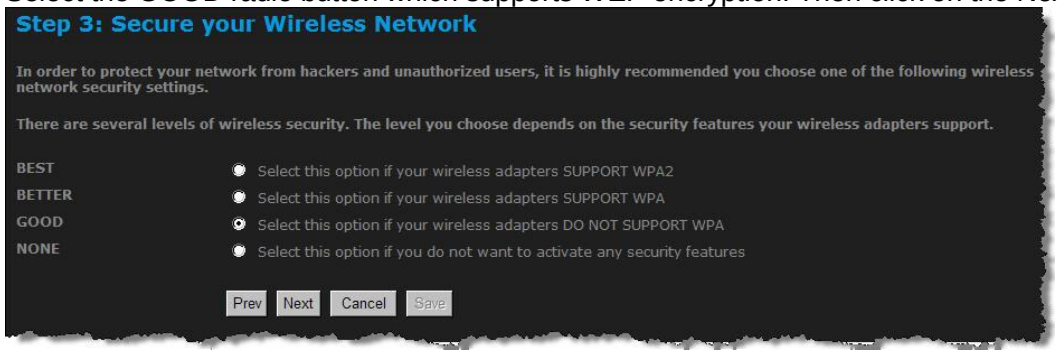
- The setup is complete. Click on the **Save** button and then reboot the device.



EnGenius®

5.1.2.3. Wireless Security Level: GOOD (WEP 64/128-bit)

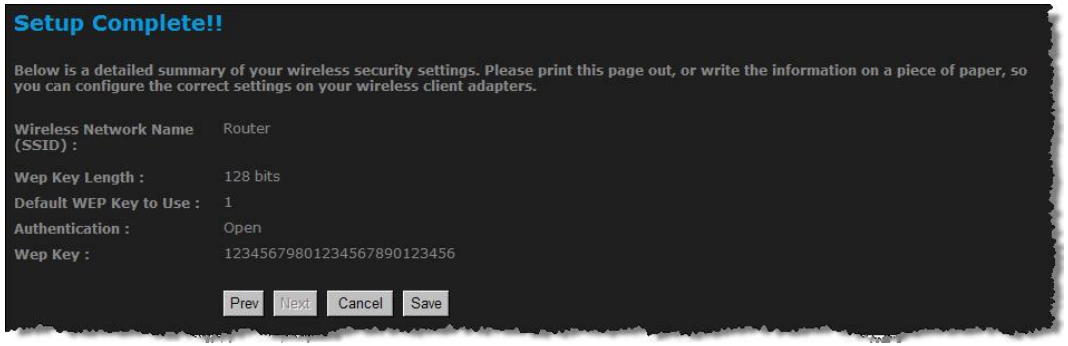
- Select the GOOD radio button which supports WEP encryption. Then click on the Next button.



- Enter a security password between 2 and 20 characters then click on the **Next** button.

- The setup is complete. Click on the **Save** button and then reboot the device.

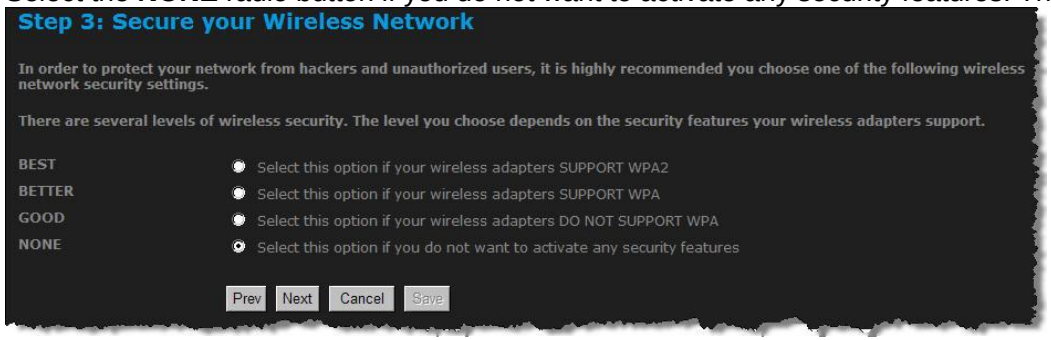
EnGenius®


Setup Complete!!
Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.
Wireless Network Name (SSID) :
Router
Wep Key Length :
128 bits
Default WEP Key to Use :
1
Authentication :
Open
Wep Key :
12345679801234567890123456
Prev
Next
Cancel
Save

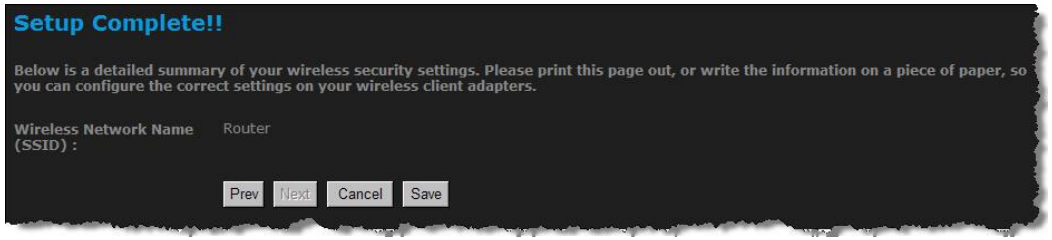
EnGenius®

5.1.2.4. Wireless Security Level: None (Security Disabled)

- Select the **NONE** radio button if you do not want to activate any security features. Then click on the **Next** button.



- The setup is complete. Click on the **Save** button and then reboot the device.

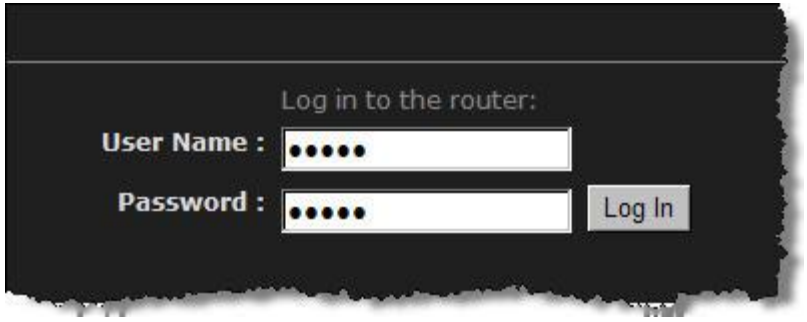


- The setup is complete. Click on the **Save** button and then reboot the device.

6. Manual Web Configuration

6.1. Logging In

- To configure the device through the web-browser, enter the IP address of the Bridge (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Enter **Admin** for both User Name and Password.



After logging in you will see the graphical user interface (GUI) of the device. The navigation tree menu on left is divided following sections:

1. **Basic**: This menu includes the wireless wizard, network settings, wireless settings, and WAN settings.
2. **Advanced**: This menu includes virtual server, special applications, port forwarding, routing, access control, web filter, MAC address filter, firewall, etc.
3. **Tools**: This menu includes time, firmware, system log, DDNS, schedules, etc.
4. **Status**: This menu displays the wireless status, logs, statistics, routing, and internet sessions.
5. **Help**: Displays the help for configuring the device.
6. **Logout**: Used to logout of the device.

6.2. Basic

Click on the **Basic** link on the navigation drop-down menu.

6.2.1. Internet Settings

Refer to Chapters 4 in order to use the wizard. The other options are described below.

6.2.2. Wizard Wireless

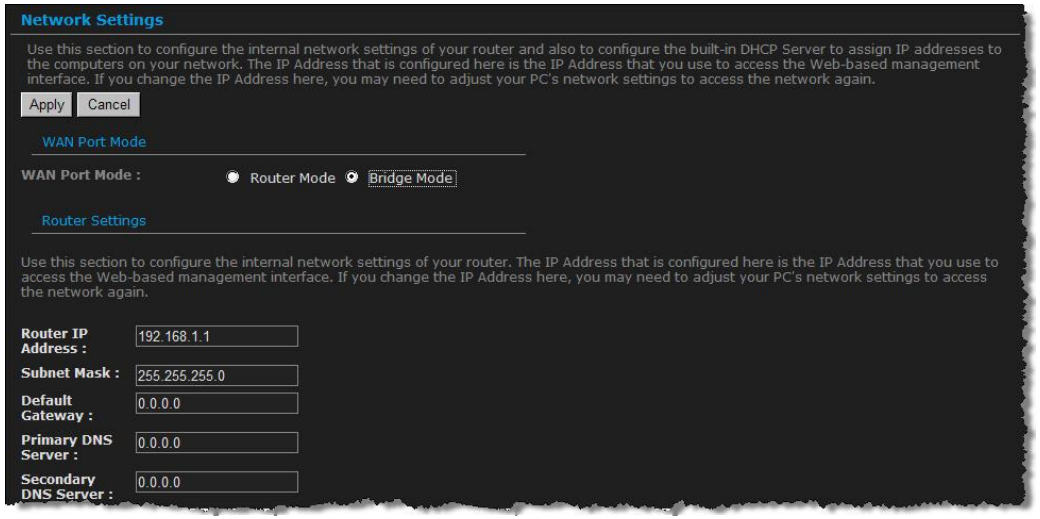
Refer to Chapters 5 in order to use the wizard. The other options are described below.

6.2.3. Network Settings

This device can be configured at a **Router** or a **Bridge**. Select Router mode if the WAN port is connected to the Internet. Select Bridge if the device is connected to a local network downstream from another router.

6.2.3.1. Bridge Mode

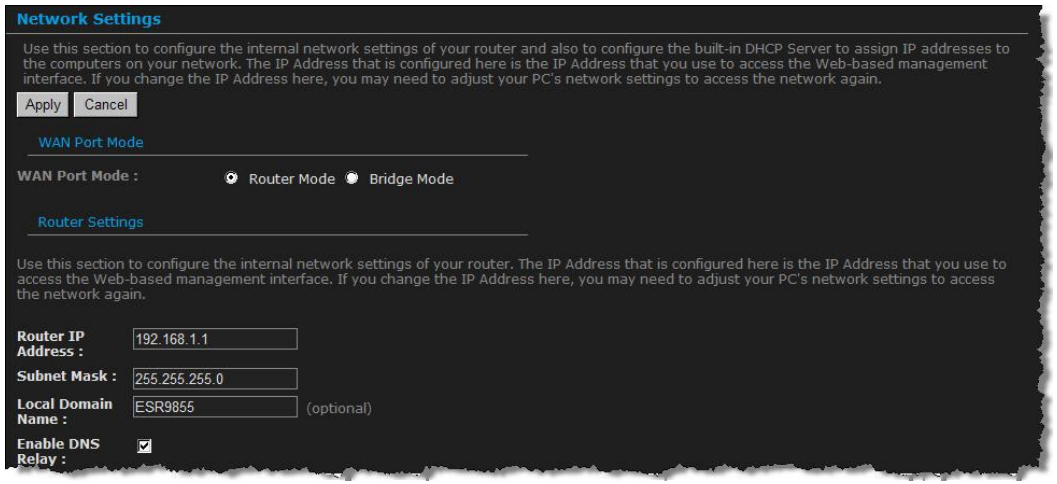
In this mode, the device functions as a bridge between the network on its WAN port and the devices on its LAN port and those connected to it wirelessly. Select the **Bridge Mode** radio button.



- **WAN Port Mode**: Select the **Bridge Mode** radio button.
- **Router IP Address**: Specify the IP address of this device.
- **Subnet Mask**: Specify the subnet mask for the IP address.
- **Default Gateway**: Specify the IP address of the upstream router.
- **Primary/Secondary DNS**: Specify the IP address of the DNS server.
- Click on the **Save Changes** button to store these settings.

6.2.3.2. Router Mode

In this mode, the device functions as a NAT router and is connected to the Internet. Select the **Router Mode** radio button.

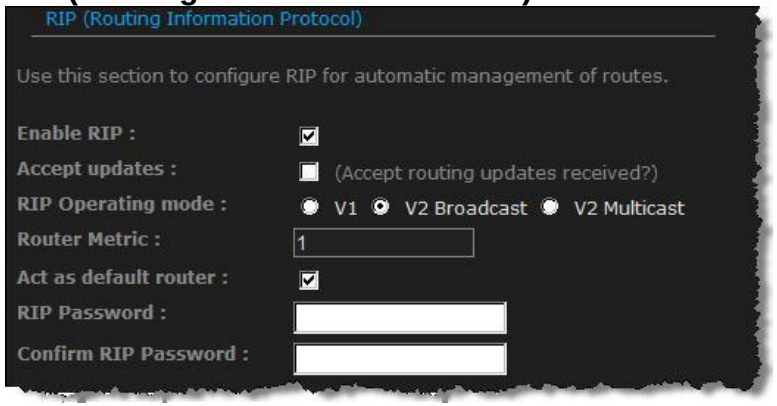


- **WAN Port Mode**: Select the **Router Mode** radio button.
- **Router IP Address**: Specify the IP address of this device
- **Subnet Mask**: Specify the subnet mask for the IP address
- **Local Domain Name**: This entry is optional. Enter a domain name for the local network. LAN computers will assume this domain name when they get an address from the router's built in DHCP server. So, for example, if you enter mynetwork.net here, and you have a LAN side laptop with a name of chris, that laptop will be known as chris.mynetwork.net. Note, however, the entered domain name can be overwritten by the one obtained from the router's upstream DHCP server.

- **Enable DNS Relay:** Place a check in this box to enable the DNS relay feature. When DNS Relay is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server.

- Click on the **Apply** button to store these settings.

RIP (Routing Information Protocol)



RIP enables the router to share routing information with other routers and hosts on the LAN.

- **Enable RIP:** Enable RIP if the LAN has multiple routers or if the LAN has other hosts that listen for RIP messages, such as auto-IP devices or the Windows XP RIP Listener Service.
- **RIP Operating mode:** This router supports both version 2 and version 1 of the RIP specification.

  V1. Use if none of the routers supports Version 2.

  V2 Broadcast. Use if some routers are capable of Version 2, but some are only capable of Version 1.

  V2 Multicast. Use if this is the only rounter on the LAN or if all the routers support Version 2.

- **Router Metric:** The additional cost of routing a packet through this router. The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes.

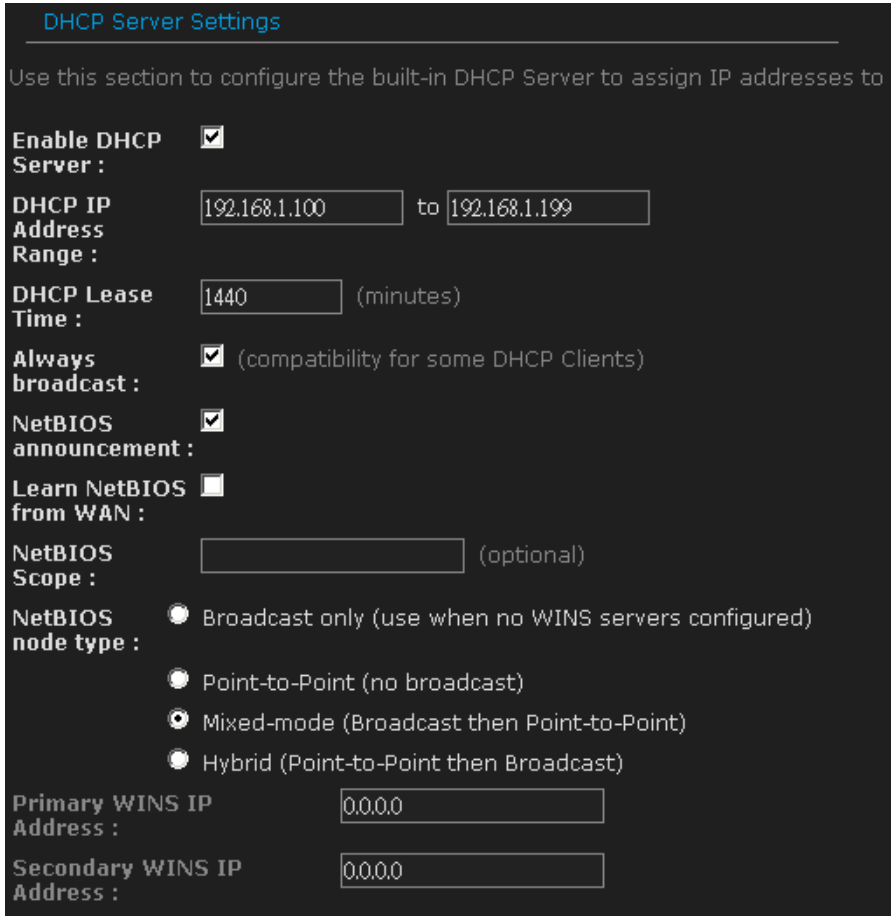
- **Act as default router:** Make this router the preferred destination for packets that are not otherwise destined.

- **RIP Password:** This router supports the use of clear-text passwords in RIP version 2 messages. Only routers with the same RIP password can share routes via RIP. RIP passwords serve more as a mechanism to limit route sharing rather than as a security mechansim. You might use RIP passwords, for example, to prevent routes from one subnet from being seen by a router on another

subnet that has conflicting IP addresses. Enter the password twice for verification. Leave both password fields empty if RIP passwords are not used.

- **Accept RIP Updates:** The "Accept RIP Updates" option controls whether the router updates its routing tables when it receives RIP messages from other LAN devices. Disable "Accept RIP Updates" if not needed or if RIP messages could originate from an insecure device on the LAN. Enable "Accept RIP Updates" only if operation of your network requires updates from other routers, and if you have assured the security of RIP messages on your network.

DHCP Server Settings



DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

- **Enable DHCP Server:** Once your router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically". When you set **Enable DHCP Server**, the following options are displayed.

- **DHCP IP Address Range:** These two IP values (*from* and *to*) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

  It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved (see DHCP Reservation below), so that the DHCP Server knows that this specific address can only be used by a specific computer or device.

  Your router, by default, has a static IP address of 192.168.0.1. This means that addresses 192.168.0.2 to 192.168.0.254 can be made available for allocation by the DHCP Server.

- **DHCP Lease Time:** The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

- **Always Broadcast:** If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

- **NetBIOS Advertisement:** Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allows LAN hosts to discover all other computers within the network, e.g. within Network Neighbourhood.

- **Learn NetBIOS information from WAN:** If NetBIOS advertisement is swicthed on, switching this setting on causes WINS information to be learned from the WAN side, if available. Turn this setting off to configure manually.

- **Primary WINS Server IP address:** Configure the IP address of the preferred WINS server. WINS Servers store information regarding network hosts, allowing hosts to 'register' themselves as well as discover other available hosts, e.g. for use in Network Neighbourhood. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

- **Secondary WINS Server IP address:** Configure the IP address of the backup WINS server, if any. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

- **NetBIOS Scope:** This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS 'domain' name under which network hosts operate. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

- **NetBIOS Registration Mode:** Indicates how network hosts are to perform NetBIOS name registration and discovery.

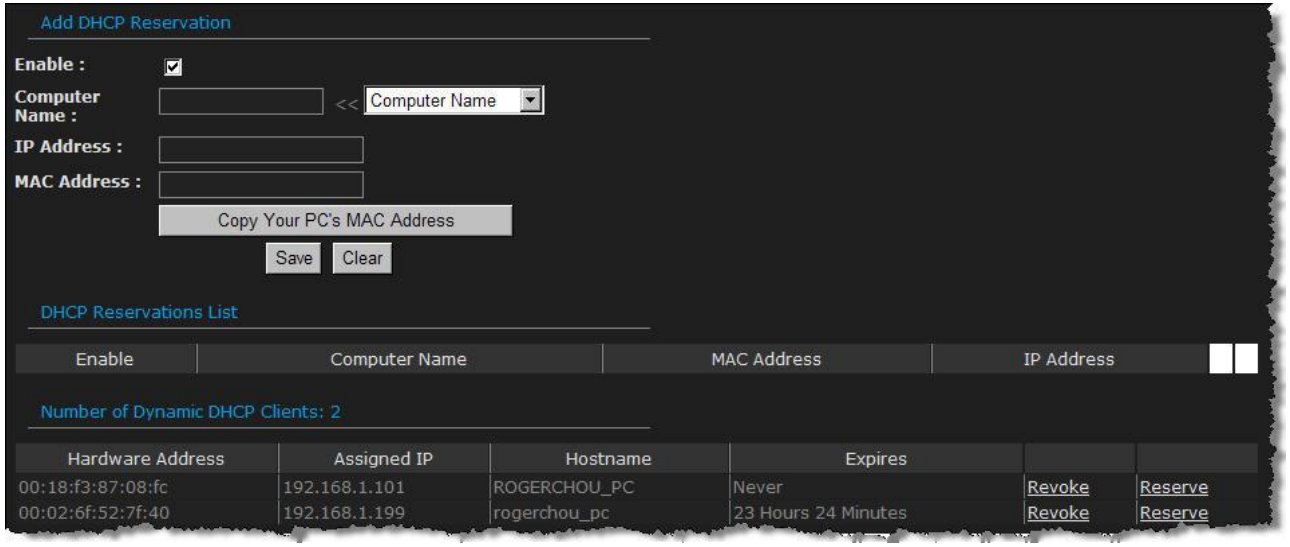
  Broadcast only: Local network broadcast only. This setting is useful where there are no WINS servers available, however, it is preferred you try Mixed Mode operation first. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

  Point-to-Point: Use WINS servers only. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server.

  Mixed Mode: First, the Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN.

  Hybrid: First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers.

Add/Edit DHCP Reservation



This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

- **Computer Name:** You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way. Example: Game Server.
- **IP Address:** The LAN address that you want to reserve.
- **MAC Address:** To input the MAC address of your system, enter it in manually or connect to the router's Web-Management interface from the system and click the Copy Your PC's MAC Address button. A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or

colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the router from the computer and click the Copy Your PC's MAC Address button to enter the MAC address.

DHCP Reservations List

This shows clients that you have specified to have reserved DHCP addresses. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit DHCP Reservation" section is activated for editing.

Number of Dynamic DHCP Clients

In this section you can see what LAN devices are currently leasing IP addresses.

Revoke: The Revoke option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed. Clicking Revoke cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

Reserve: The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

6.2.4. Wireless Settings

These options allow you to enable/disable the wireless interface, switch between the 11b, 11g, 11n and mixed radio band and channel frequency

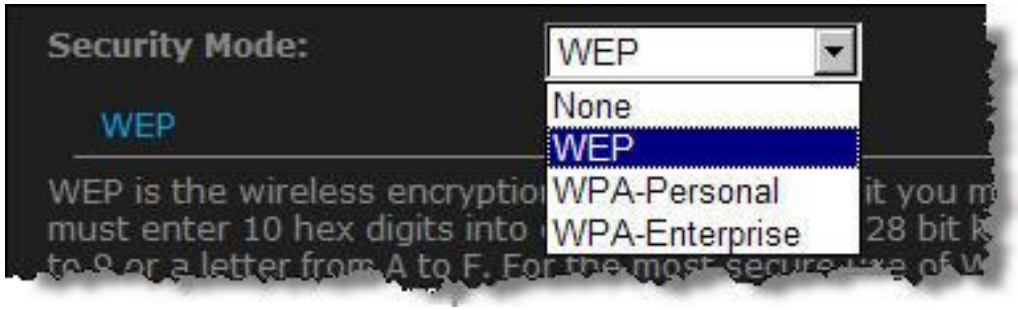
- **Enable Wireless:** Place a check in this box to enable the wireless interface, it is enabled by default.
- **Wireless Network Name**: The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters.
  - **802.11 Mode**: Select the IEEE 802.11 mode from the drop-down list. For example, if you are certain that the wireless network will be using only IEEE 802.11g clients, then it is recommended to select **802.11g** only instead of **2.4 GHz B+G** which will reduce the performance of the wireless network. You may also select **Mixed 802.11n, 802.11g and 802.11b**. If all of the wireless devices you want to connect with this router can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

- **Wireless Channel**: Select a channel from the drop-down list. The channels available are based on the country's regulation. A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

- **Transmission Rate**: Select a transmission rate from the drop-down list. It is recommended to use the **Best (automatic)** option.
- **Channel Width**: Select a channel width from the drop-down list.
- **Visibility Status**: Select **Visible** or **Invisible**. This is the SSID broadcast feature. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **Show Active Clients**: Click on this button to view a list of clients that are associated with this device.
- Click on the **Save Changes** button to store these settings.

6.2.4.1. Wireless Security Mode

To protect your privacy this mode supports several types of wireless security: WEP WPA, WPA2, and WPA-Mixed. WEP is the original wireless encryption standard. WPA provides a higher level of security. The following section describes the security configuration in detail.

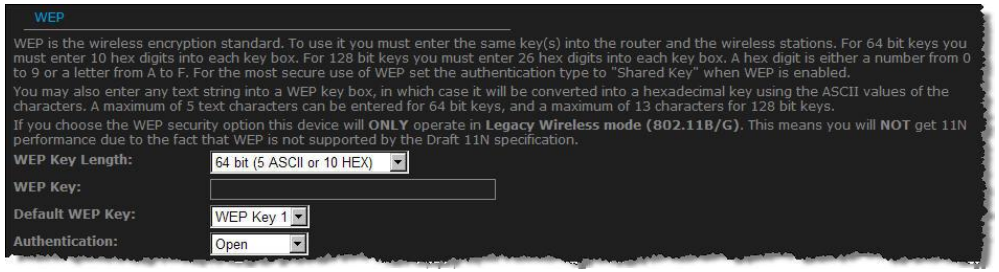


6.2.4.2. WEP (Wired Equivalent Privacy)

Select the **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length.

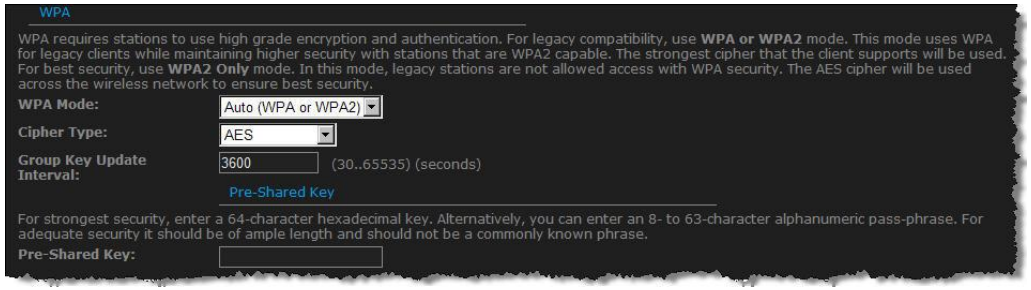
128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.



- **WEP Key Length**: Select a **64-bit** or **128-bit** WEP key length from the drop-down list.
- **WEP Key 1-4:** You may enter four different WEP keys.
- **Default WEP Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Authentication:** Select **Open**, or **Shared Key**. Authentication method from the drop-down list. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- Click on the **Save Changes** button to store these settings.

6.2.4.3. WPA Personal (Wi-Fi Protected Access)

Select the **WPA-Personal** from the drop-down list if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

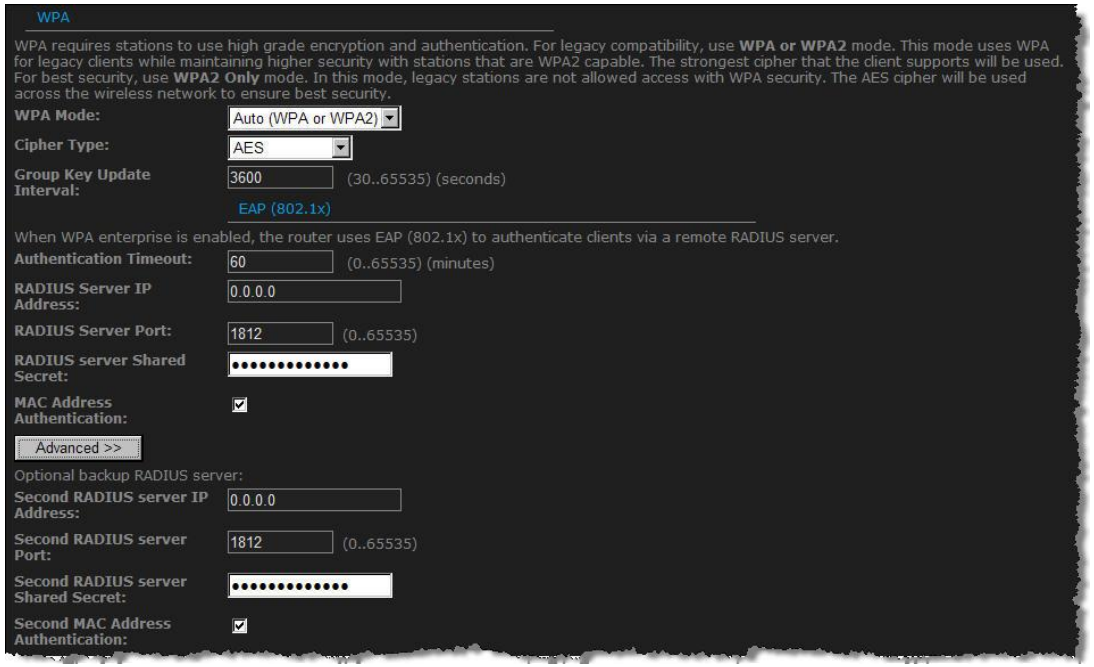


- **WPA Mode**: Select the **Auto WPA / WPA2** from the drop-down list.
- **Cipher Type**: Select **TKIP and AES** as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval**: Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Pre-Shared Key**: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.
- Click on the **Save Changes** button to store these settings.

6.2.4.4. WPA Enterprise (Wi-Fi Protected Access & 802.1x)

Select the WPA-Enterprise from the drop-down list if your wireless network uses WPA encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

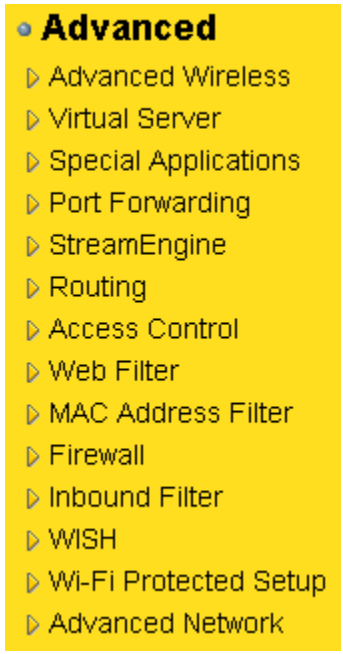
This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.



EnGenius®

- **WPA Mode**: Select the WPA / WPA2 from the drop-down list.
- **Cipher Type**: Select TKIP or AES as the cipher suite. The encryption algorithm used to secure the data communication. TKIP. Use TKIP only. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES. Use AES only. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES. TKIP and AES. The bridge negotiates the cipher type with the access point, and uses AES when available.
- **Group Key Update Interval**: Specify the number of seconds before the group key used for broadcast and multicast data is changed.
- **Authentication Timeout**: Specify the number of minutes after which the client will be required to re-authenticate.
- **RADIUS Server IP Address**: Specify the IP address of the RADIUS server.
- **RADIUS Server Port**: Specify the port number of the RADIUS server, the default port is 1812.
- **RADIUS Server Shared Secret**: Specify the pass-phrase that is matched on the RADIUS Server.
- **MAC Address Authentication:** Place a check in this box if you would like the user to always authenticate using the same computer.
- Optional Backup RADIUS server: This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding.
- Click on the **Save Changes** button to store these settings.

6.3. Advanced



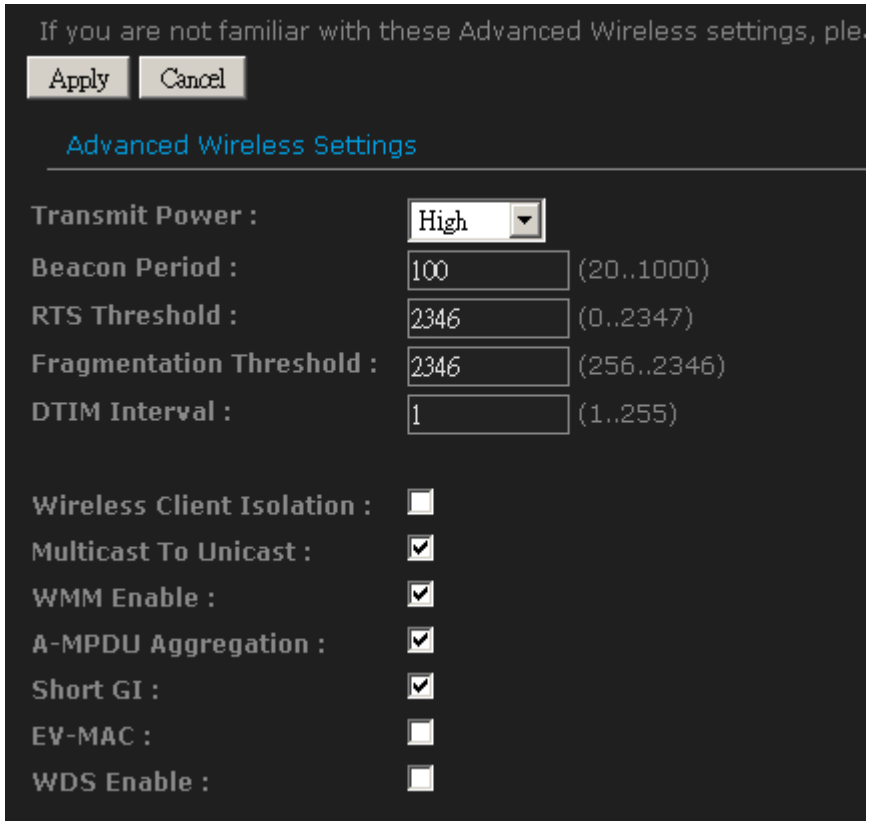
Click on the **Advanced** link on the navigation tree menu.

The configuration steps for each option are described below.

6.3.1. Advanced Wireless

By clicking on **Advanced** tab, you will be able to access Advanced Wireless page.

If you are not familiar with **Advanced Wireless Settings**, please read the help section before attempting to modify these settings.

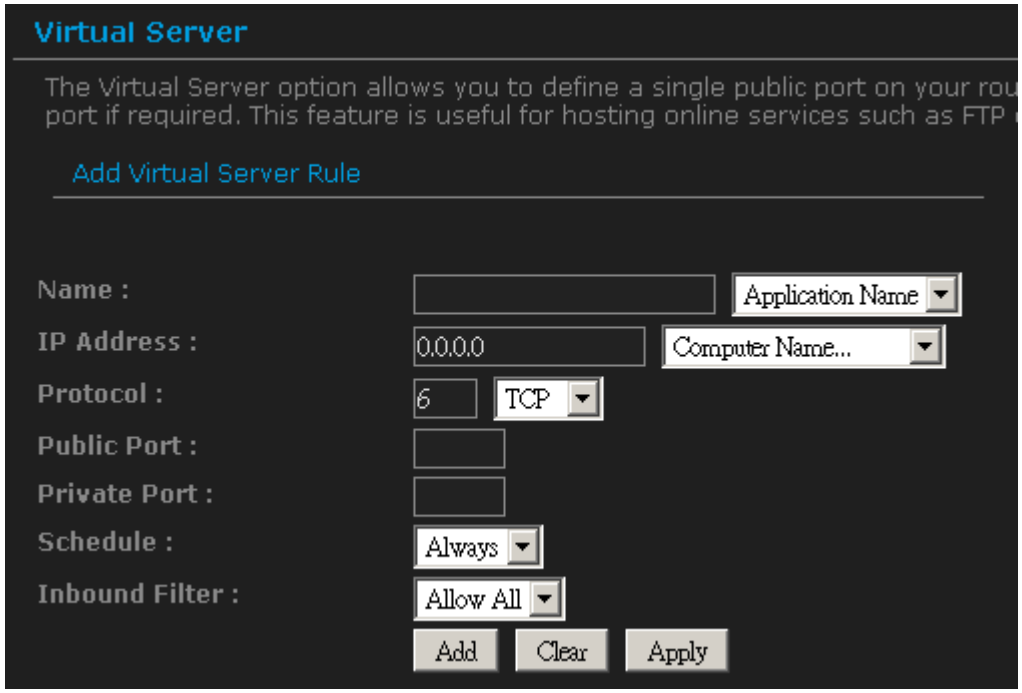


- **Transmit Power:** Set the power output of the wireless signal

- **Beacon Period:** Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds. Values that are not a multiple of 4, are forced to a multiple of 4.
- **RTS Threshold:** When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes.
- **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- **DTIM Interval:** A Delivery Traffic Indication Message informs all wireless clients that the access point will be sending Multi-cast data.
- **Wireless Client Isolation:** Enabling Wireless Client Isolation (also known as L2 Isolation) prevents associated wireless clients from communicating directly with each other by using low-level (link layer) protocols and without passing through the router.
- **Muticast to Unicast:** When multiple wireless clients are receiving streaming media, enabling this option can provide better performance in some cases by transforming each multicast packet into multiple unicast packets. (Broadcast packets are still sent out as broadcast packets.) If you experience interoperability problems when the AP is sending streaming media to some legacy wireless clients, try turning this option off.
- **WMM Enable:** Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
- **A-MPDU Aggregation:** Aggregation of wireless packets based on MAC protocol data units is a technique for maximizing performance. This option should normally remain enabled.
- **Short GI:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **EV-MAC:** Enable EV-MAC option for superior experience of wireless video streaming.
- **WDS Enable:** Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP. Enter a MAC address for each of the other APs that you want to connect with WDS.
-

6.3.2. Virtual Server

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port.

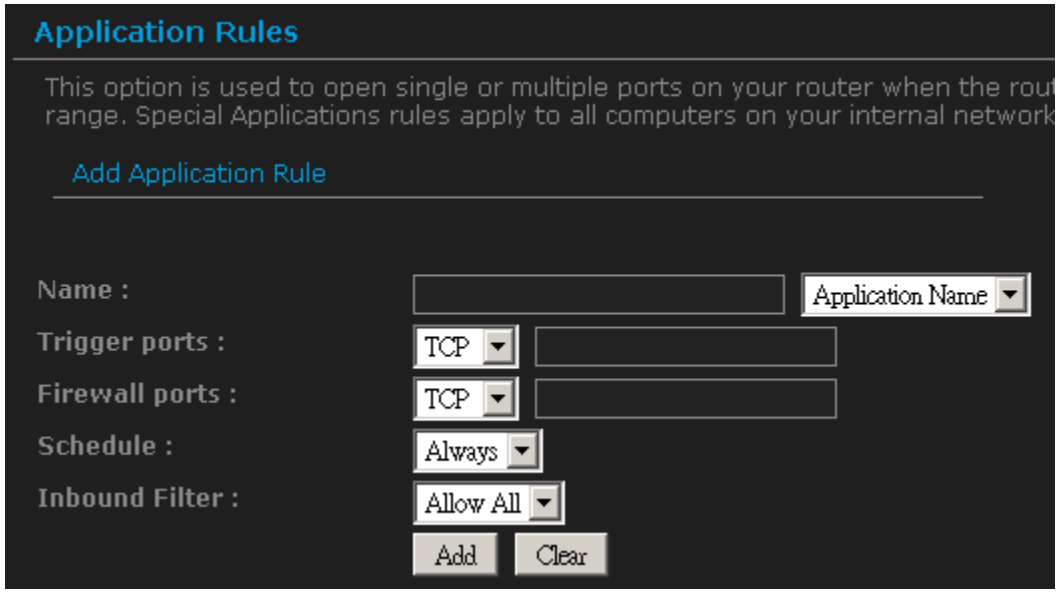


- **Name**: Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the **Application Name** drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **IP Address**: Specify the IP address for the virtual server entry.
- **Protocol**: Specify a protocol or select one from the drop-down list.

- **Public Port**: Specify the public port number.
- **Private Port**: Specify the private port number.
- **Schedule**: Select a schedule to **Always** or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- **Inbound Filter**: Select an inbound filter from the drop-down list. If an inbound filter does not exist, you may create it from Advanced > Inbound Filter section.
- Click on the **Add** button to insert the entry into the Virtual Server list.

6.3.3.Special Applications

An application rule is used to open single or multiple ports on your router when the router senses data sent to the Internet on a trigger port or port range. An application rule applies to all computers on your internal network.

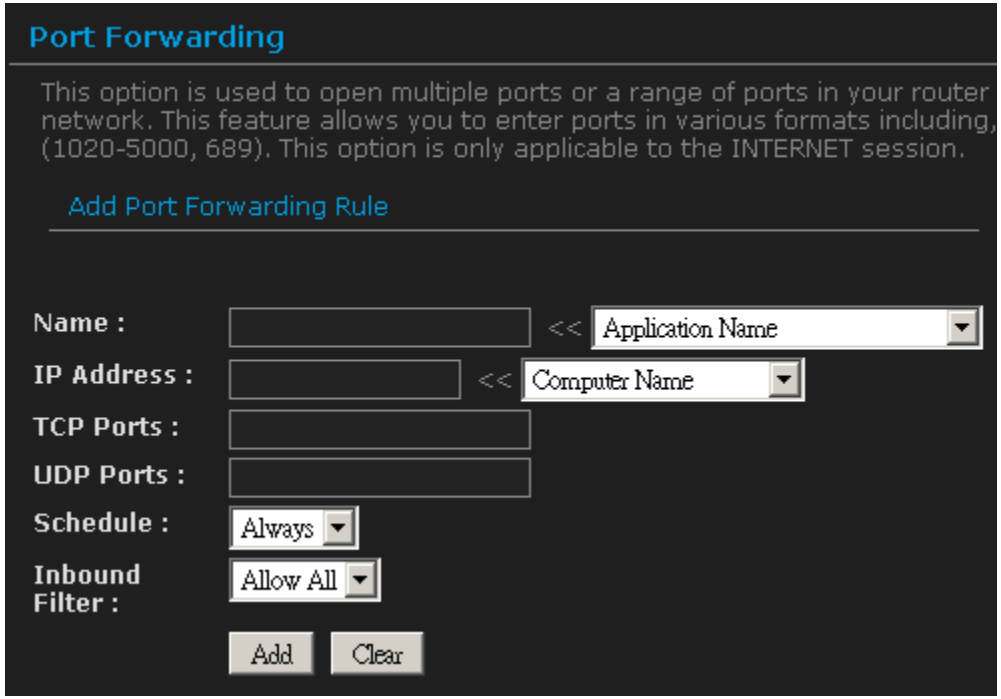


- **Name**: Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the **Application Name** drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **Triggering Ports**: Specify the outgoing port range that is used by the application.
- **Firewall Ports**: Specify the port range that you would like to open for Internet traffic.
- **Schedule**: Select a schedule to **Always** or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.
- Click on the **Add** button to insert the entry into the Special Applications list.

EnGenius®

6.3.4.Port Forwarding

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.

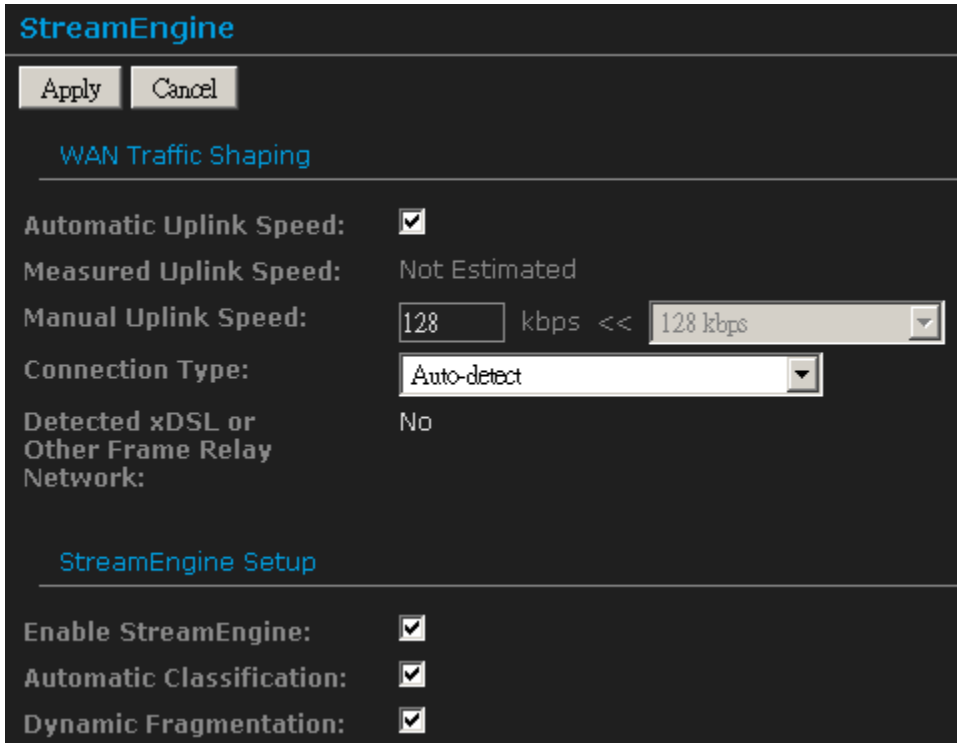


- **Name**: Assign a meaningful name to the virtual server, for example Web Server. Several well-known types of virtual server are available from the Application Name drop-down list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.
- **IP Address**: Specify the IP address for the virtual server entry.
- **TCP/UDP Ports**: Specify the TCP or UDP port numbers.
- **Schedule**: Select a schedule to **Always** or **Never** from the drop-down list. If a schedule does not exist, you may create it in the Tools > Schedule section.

- **Inbound Filter**: Select an inbound filter from the drop-down list. If an inbound filter does not exist, you may create it from Advanced > Inbound Filter section.
- Click on the **Add** button to insert the entry into the Port Forwarding list.

6.3.5.StreamEngine

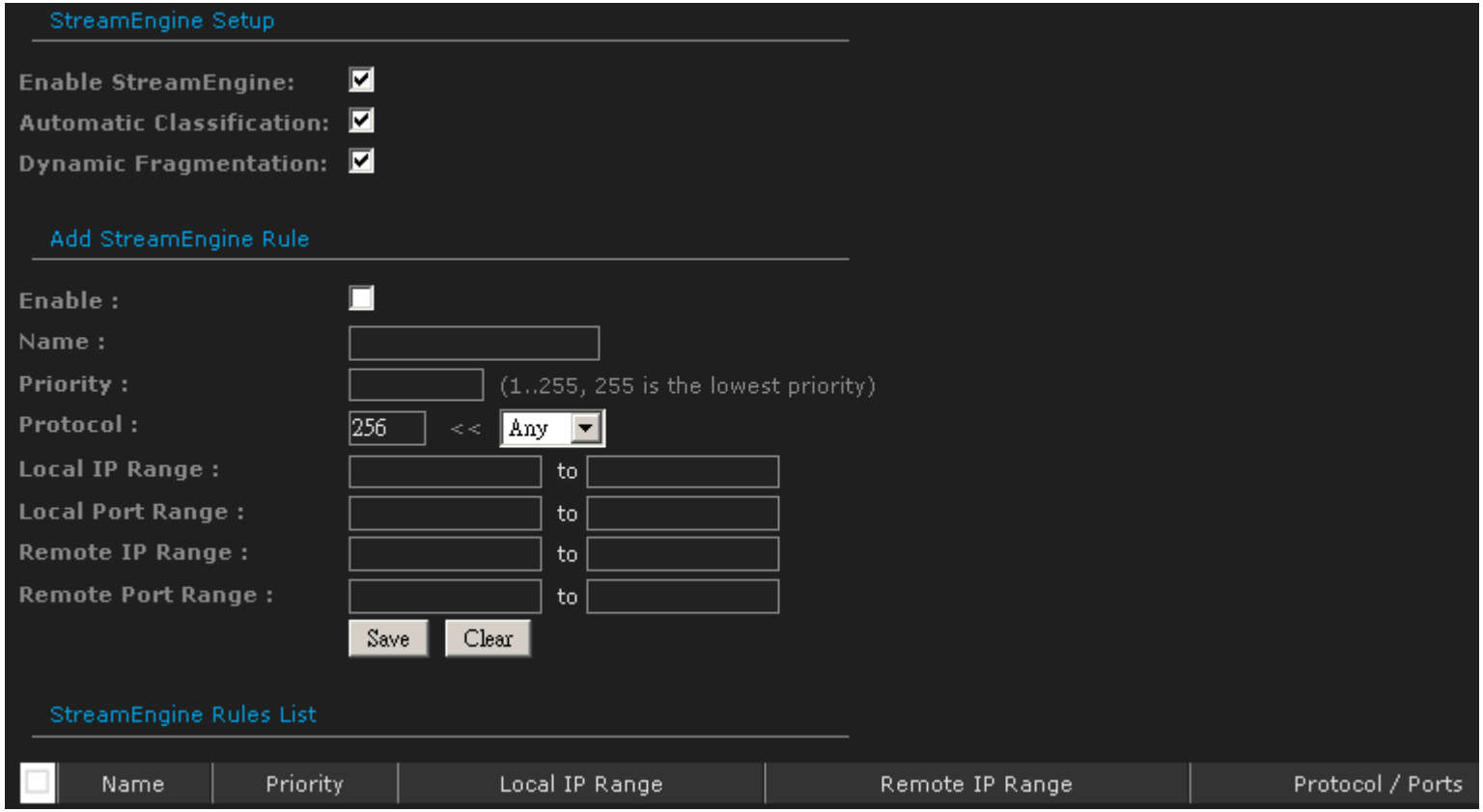
The StreamEngine feature helps improve the network performance by prioritizing applications.



- **Enable Traffic Shaping**: Place a check in the box to enable traffic shaping. When this option is enabled, the router restricts the flow of outbound traffic so as not to exceed the WAN uplink bandwidth.
- **Automatic Uplink Speed**. Place a check in this box to enable automatic uplink speed. When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).
- **Measured Uplink Speed**: Displays the uplink speed. This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads

associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.

- **Manual Uplink Speed**: Specify an uplink speed or select it from the drop-down list. If Automatic Uplink Speed is disabled, this options allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP.
- **Connection Type**: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either Static or DHCP in the WAN settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.
- Click on the **Apply** button to store these settings.



- **Enable StreamEngine**: Place a check in this box to enable this option. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.
- **Automatic Classification**: Place a check in this box to enable this option. This option is enabled by default so that your router will automatically determine which programs should have network priority.
- **Dynamic Fragmentation**: Place a check in this box to enable this option. This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.

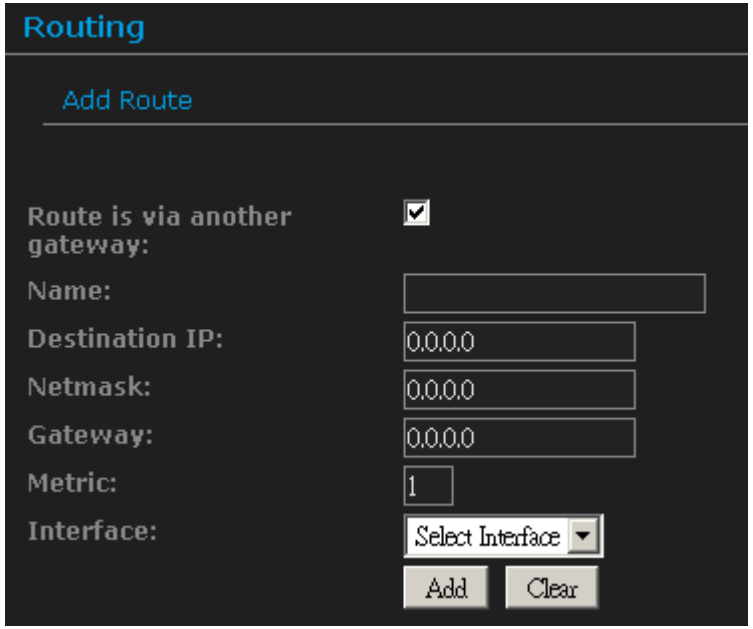
EnGenius®

- **Add StreamEngine Rule**: A StreamEngine Rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate, and specific StreamEngine Rules will not be required. StreamEngine supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match the rule with the highest priority will be used.

- **Enable**: Place a check in this box to enable the StreamEngine rule.
- **Name**: Specify a name for the rule.
- **Priority**: Specify a priority for the rule. Being with 1 which is the highest and 255 the lowest priority.
- **Protocol**: Specify a protocol or select one from the drop-down list.
- **Local IP Range**: Specify the local (LAN) IP address range.
- **Local Port Range**: Specify the local (LAN) port range.
- **Remote IP Range**: Specify the remote (WAN) IP address range.
- **Remote Port Range**: Specify the remote (WAN) port range.
- Click on the **Save** button to insert the entry into the StreamEngine list.

6.3.6.Routing

This section adds a new entry into the routing table.

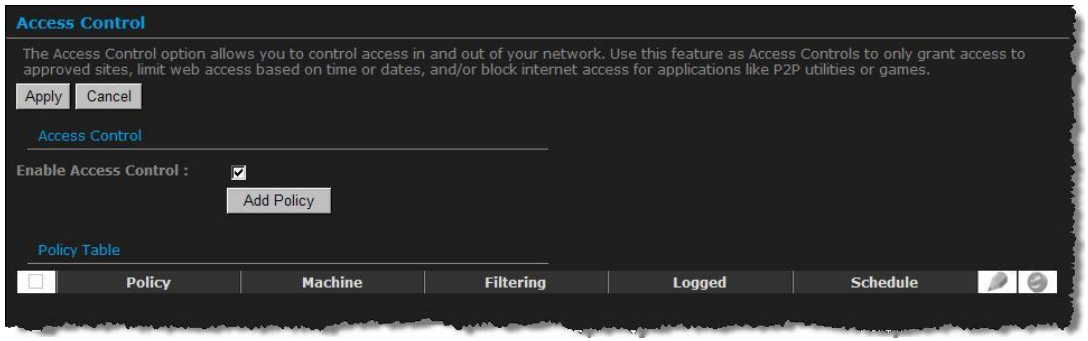


- **Name**: Specify a name for the rule.
- **Destination IP**: Specify the destination IP address.
- **Netmask**: Specify the subnet mask for the IP address.
- **Gateway**: Specify the IP address of the gateway.
- **Metric**: Specify the number of routing hops. The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.
- **Interface**: Select the interface from the drop-down list.
- Click on the **Add** button to insert the entry into the Routing table.

6.3.7. Access Control

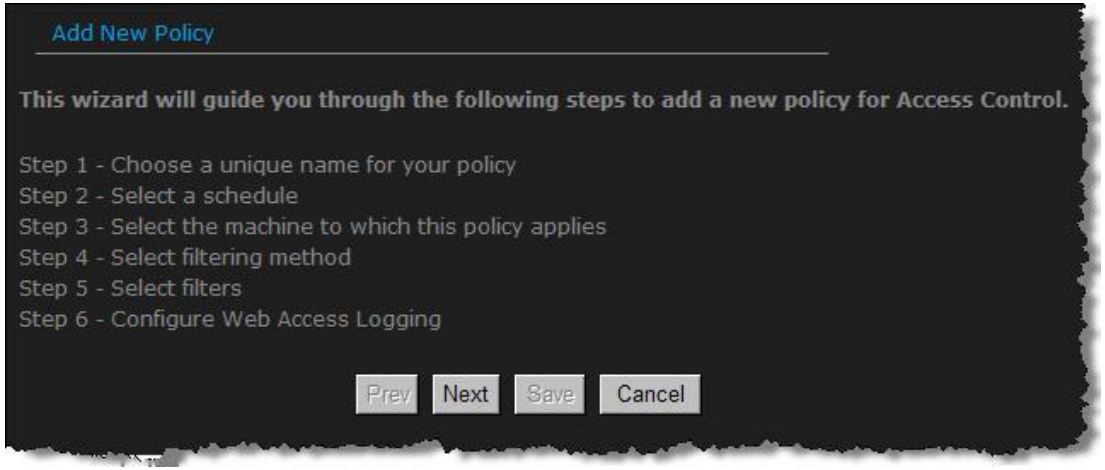
The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.

When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.

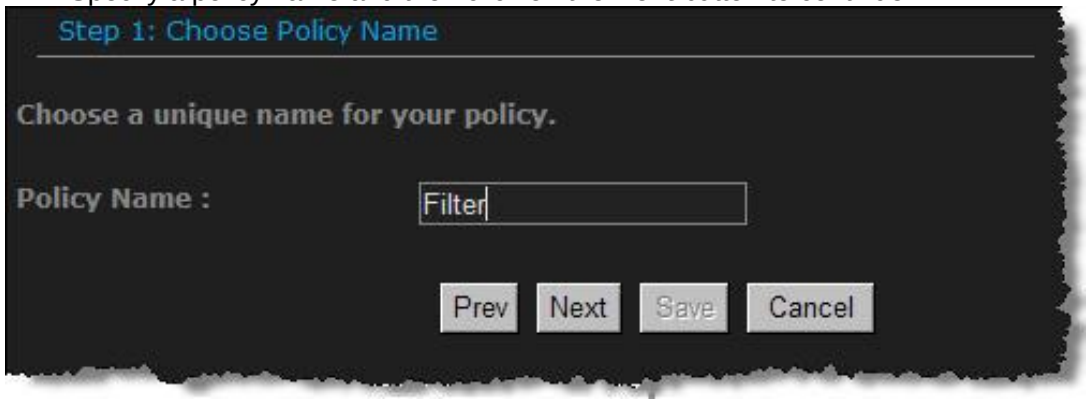


- Place a check in the **Enable Access Control** check box and then click on the **Add Policy** button. This will bring up the **Add New Policy** wizard.
- The wireless wizard will inform you that there are six major steps in the process.
- Choose a unique name for your policy
- Select a schedule
- Select the machine to which the policy applies
- Select filtering method
- Configure web access logging

- Click on the **Next** button to continue.

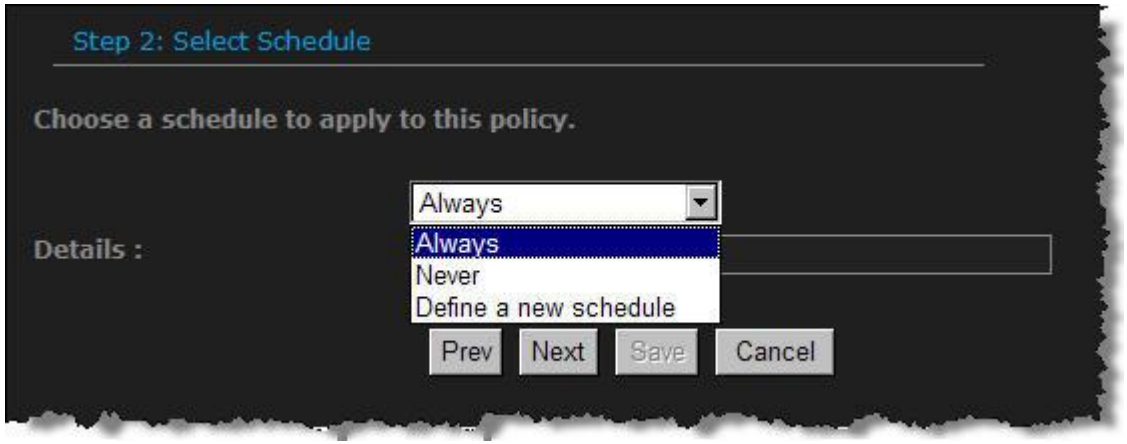


- Specify a policy name and then click on the **Next** button to continue.

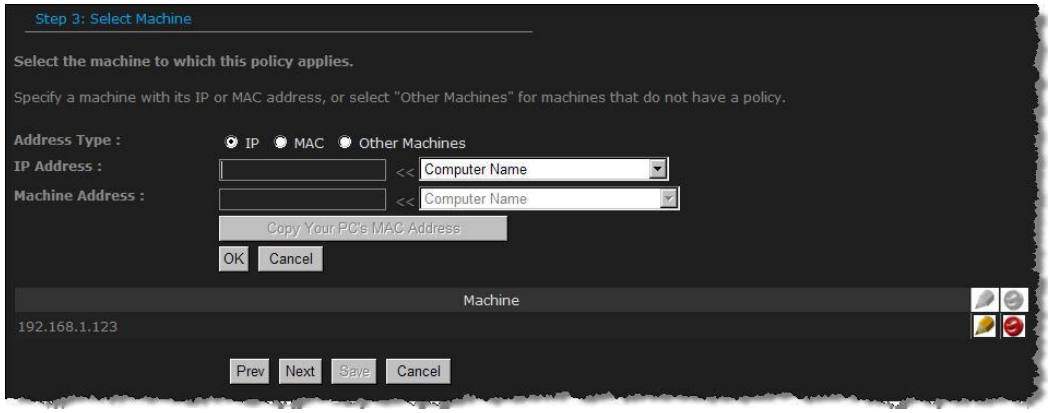


- Select a schedule from the drop-down list: **Always** or **Never**, or you may define a new schedule. Click on the **Next** button to continue.

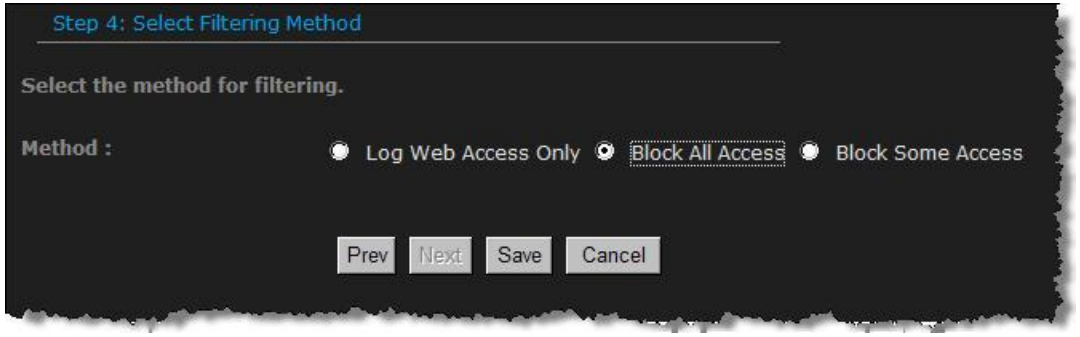
EnGenius®



- Select a machine to which the policy applies.
- **Address Type**: Select the IP address or MAC address radio button.
- **IP Address**: If you selected IP address above, then specify the IP address here.
- **MAC Address**: If you need to change the MAC address of the rounter's WAN-side Ethernet interface, either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or click on **Clone Your PCs MAC Address**.
- Click on the **OK** button to insert the entry into the table.
- Click on the **Next** button to continue.



- Select a filtering method:
- **Log Web Access Only**: Select this radio but in order to log web access.
- **Block All Access**: Select this radio but in order to block all web access.
- **Block Some Access**: Select this radio but in order to block some web access.
- Click on the **Save** button to store the changes.



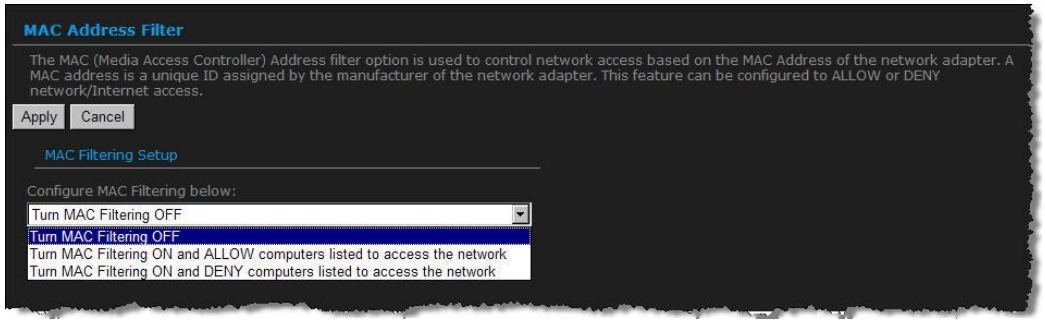
6.3.8.Web Filter

This is a type of parental control feature used to restrict certain websites form being accessed through your network. These filters can be used for securing and restricting your network.

Website/URL/Domain: Specify the web address that you would like to filter. **Do not use "http://"**
Click on the **Save** button to store the changes.

6.3.9.MAC Address Filter

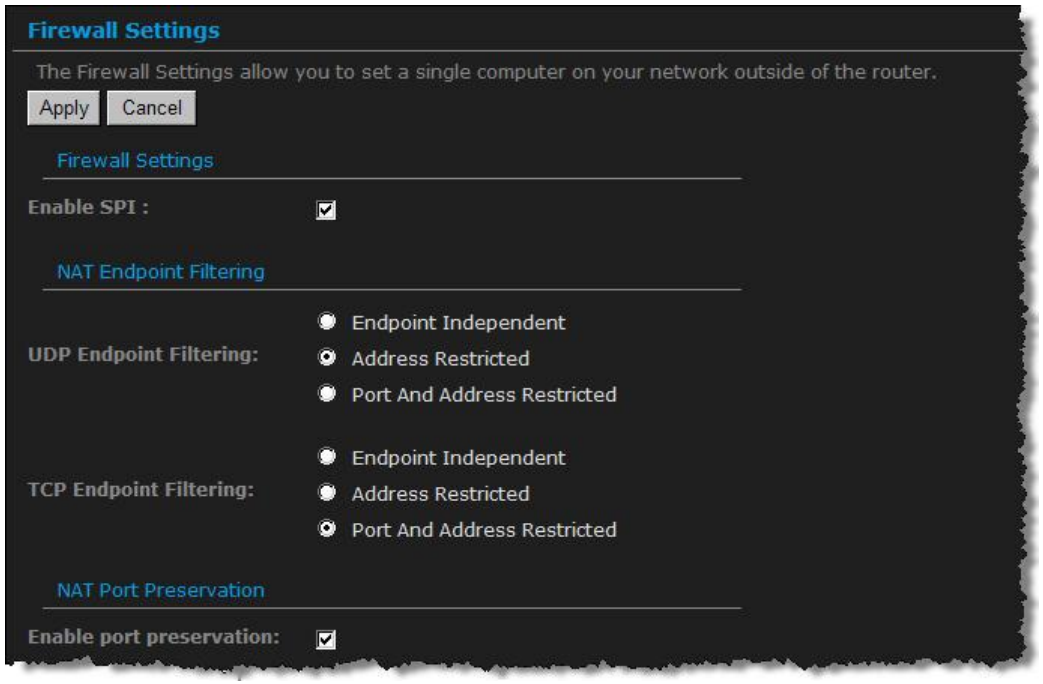
This feature is used to restrict certain MAC address from accessing the Internet. These filters can be used for securing and restricting your network.



- **Configure MAC Filtering**: Select one of the options from the drop-down list.
- **Turn MAC Filtering OFF:** When "OFF" is selected, MAC addresses are not used to control network access.
- **Turn MAC Filtering ON and ALLOW computers listed to access the network:** When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Filtering Rules list are granted network access.
- **Turn MAC Filtering ON and DENY computers listed to access the network:** When "DENY" is selected, any computer with a MAC address listed in the MAC Filtering Rules list is refused access to the network.
- **MAC Address**: Specify that MAC address that you would like to filter.
- Click on the **Save** button to store the changes.

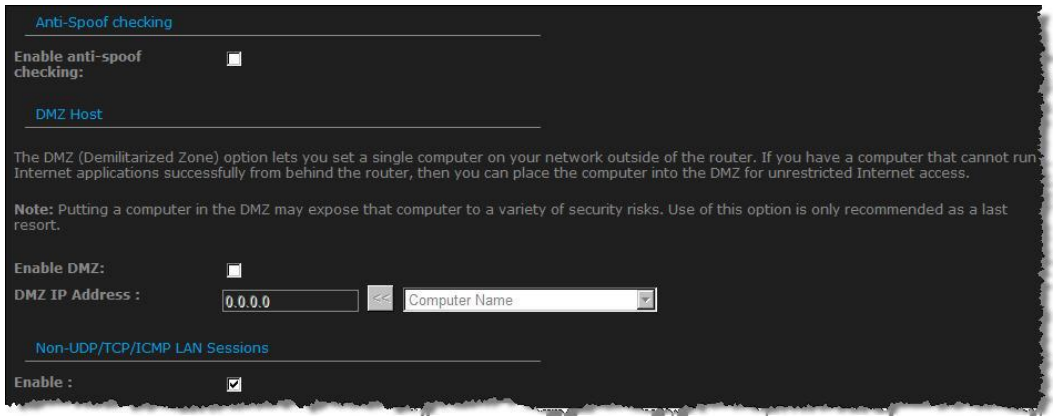
6.3.10. Firewall

The device provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attacks. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.



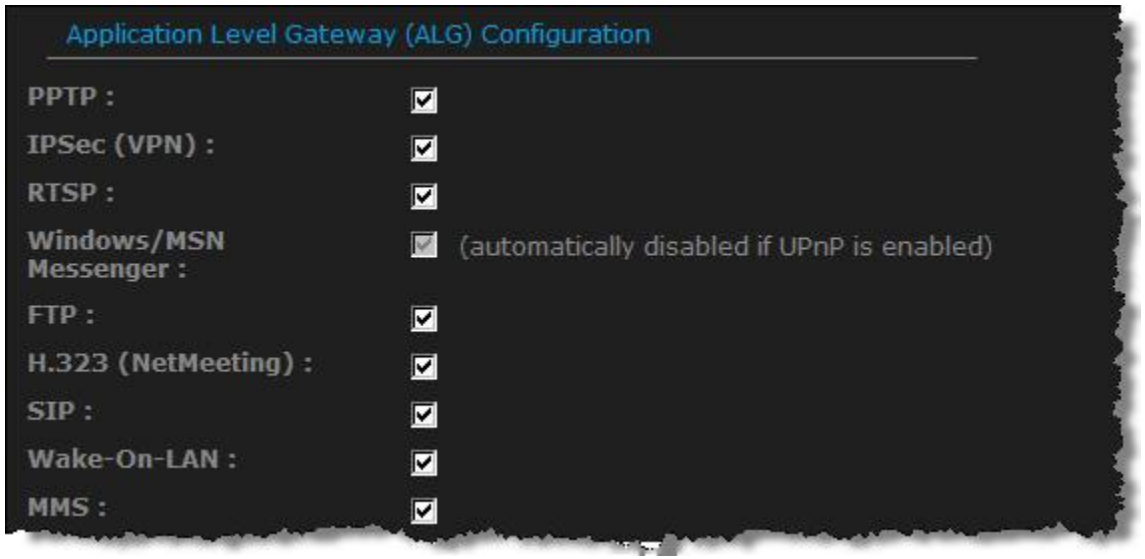
- **Enable SPI**: Place a check in this box to enable SPI. SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol. When the protocol is TCP, SPI checks that packet sequence numbers are within the valid range for the session, discarding those packets that do not have valid sequence numbers. Whether SPI is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state.

- **TCP / UDP NAT Endpoint Filtering** options control how the router's NAT manages incoming connection requests to ports that are already being used. Select one of the radio buttons.
- **End Point Independent** Once a LAN-side application has created a connection through a specific port, the NAT will forward any incoming connection requests with the same port to the LAN-side application regardless of their origin. This is the least restrictive option, giving the best connectivity and allowing some applications (P2P applications in particular) to behave almost as if they are directly connected to the Internet.
- **Address Restricted** The NAT forwards incoming connection requests to a LAN-side host only when they come from the same IP address with which a connection was established. This allows the remote application to send data back through a port different from the one used when the outgoing session was created.
- **Port And Address Restricted** The NAT does not forward any incoming connection requests with the same port address as an already establish connection.
- **Note**: Some of these options can interact with other port restrictions. Endpoint Independent Filtering takes priority over inbound filters or schedules, so it is possible for an incoming session request related to an outgoing session to enter through a port in spite of an active inbound filter on that port. However, packets will be rejected as expected when sent to blocked ports (whether blocked by schedule or by inbound filter) for which there are no active sessions. Port and Address Restricted Filtering ensures that inbound filters and schedules work precisely, but prevents some level of connectivity, and therefore might require the use of port triggers, virtual servers, or port forwarding to open the ports needed by the application. Address Restricted Filtering gives a compromise position, which avoids problems when communicating with certain other types of NAT router (symmetric NATs in particular) but leaves inbound filters and scheduled access working as expected.
- **Enable Port Preservation**: Place a check in this box to enable Port Preservation. NAT Port preservation (on by default) tries to ensure that, when a LAN host makes an Internet connection, the same LAN port is also used as the Internet visible port. This ensures best compatibility for internet communications. Under some circumstances it may be desirable to turn off this feature.



EnGenius®

- **Enable anti-spoof checking**: Place a check in this box to enable anti-spoof checking. Enabling this option can provide protection from certain kinds of "spoofing" attacks. However, enble this option with care. With some modems, the WAN connection may be lost when this option is enabled. In that case, it may be necessary to change the LAN subnet to something other than 192.168.0.x (192.168.2.x, for example), to re-establish the WAN connection.
- **Enable DMZ Host**: Place check in this box to enable DMZ host. DMZ host is a demilitarized zone used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web, FTP, email and DNS servers.
- **DMZ IP Address**: Specify the IP address of the DMZ host.
- **Non-UDP/TCP/ICMP LAN Sessions**: Place a check in this box to enable this feature. When a LAN application that uses a protocol other than UDP, TCP, or ICMP initiates a session to the Internet, the router's NAT can track such a session, even though it does not recognize the protocol. This feature is useful because it enables certain applications (most importantly a single VPN connection to a remote host) without the need for an ALG.
- **Note**: This feature does not apply to the DMZ host (if one is enabled). The DMZ host always handles these kinds of sessions.
- Enabling this option (the default setting) enables single VPN connections to a remote host. (But, for multiple VPN connections, the appropriate VPN ALG must be used.) Disabling this option, however, only disables VPN if the appropriate VPN ALG is also disabled.



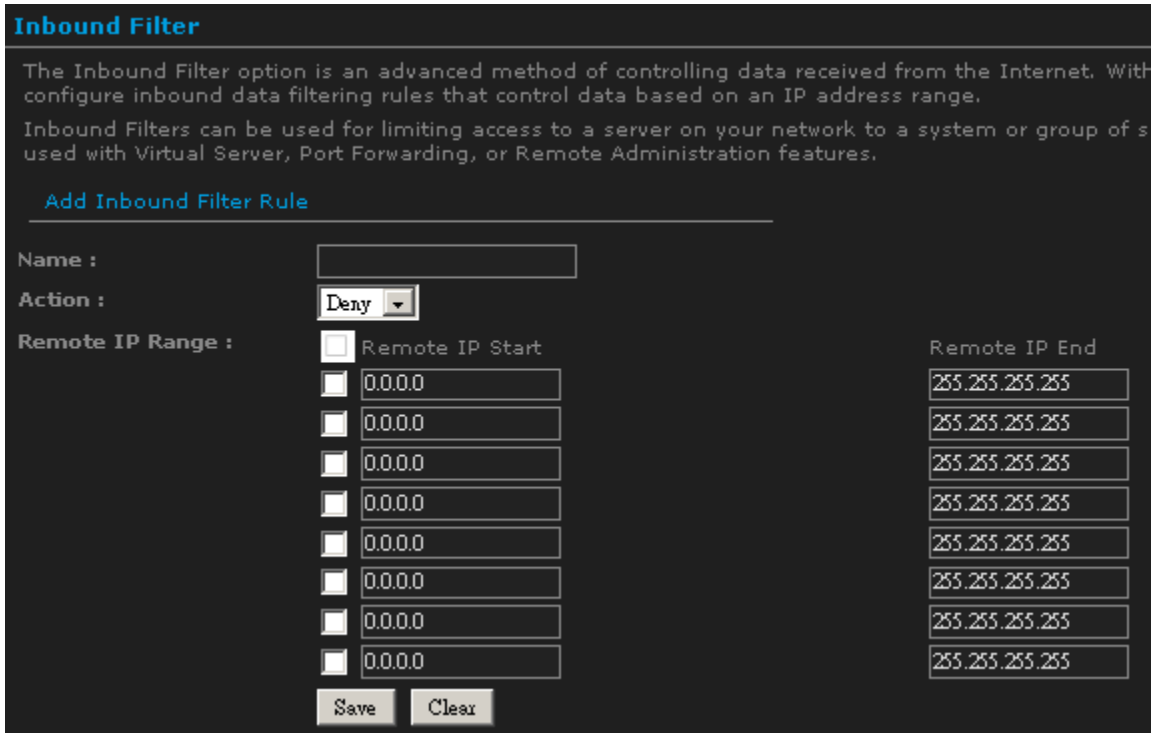
EnGenius®

- **Application Layer Gateway (ALG)** Configuration: Place a check in appropriate feature boxes to enable them. . Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.
- **PPTP**: Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the PPTP ALG is to increase VPN performance. Enabling the PPTP ALG also allows incoming VPN connections to a LAN side VPN server (refer to Advanced → Virtual Server).
- **IPSec**: (VPN) Allows multiple VPN clients to connect to their corporate networks using IPSec. Some VPN clients support traversal of IPSec through NAT. This option may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try disabling this option. Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.
- **RTSP**: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.
- **Windows/MSN Messenger**: Supports use on LAN computers of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) and MSN Messenger. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled.
- **FTP**: Allows FTP clients and servers to transfer data across NAT.
- **H.323 (Netmeeting)**: Allows H.323 (specifically Microsoft Netmeeting) clients to communicate across NAT server.
- **SIP**: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.
- **Wake-On-LAN**: This feature enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable.
- **MMS**: Allows Windows Media Player, using MMS protocol, to receive streaming media from the internet.
- Click on the **Apply** button to store these settings.

6.3.11. Inbound Filter

When you use the Virtual Server, Port Forwarding, or Remote Administration features to open specific ports to traffic from the Internet, you could be increasing the exposure of your LAN to cyber attacks from the Internet. In these cases, you can use Inbound Filters to limit that exposure by specifying the IP addresses of internet hosts that you trust to access your LAN through the ports that you have opened.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features.

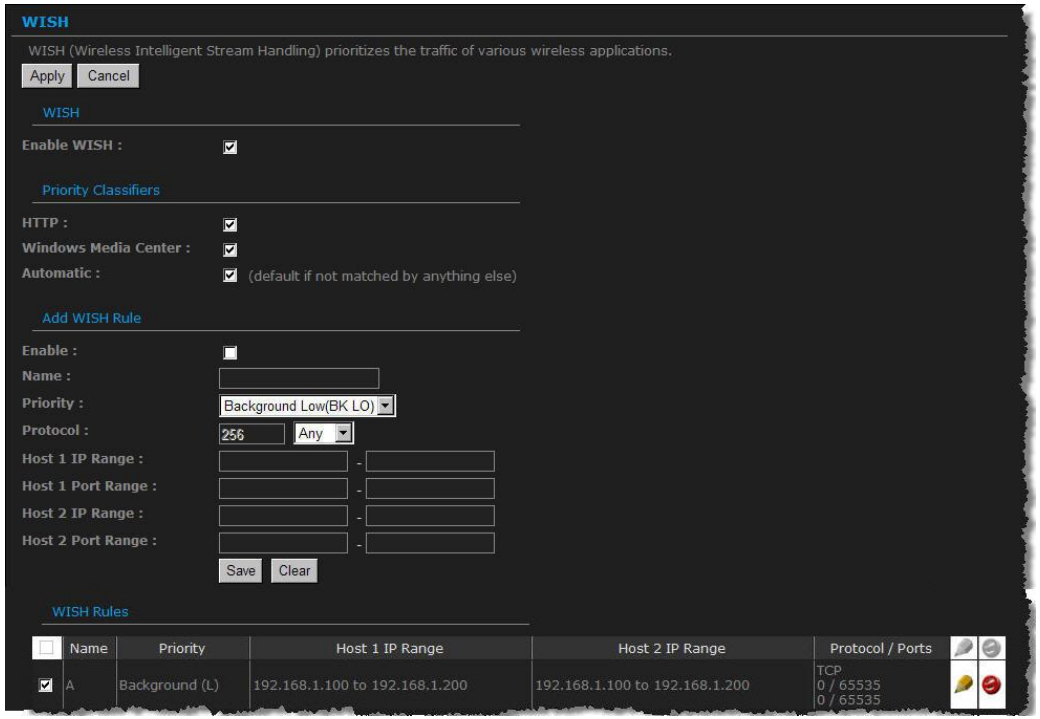


- **Name** Specify a name for the inbound filter.

- **Action:** Select Allow or Deny from the drop-down list. This will apply the inbound filter rule on the WAN interface.
- **Remote IP Range:** Specify the remote IP address range and then click in the check box to enable the range.
- Click on the **Save** button to store the changes.

6.3.12. WISH

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

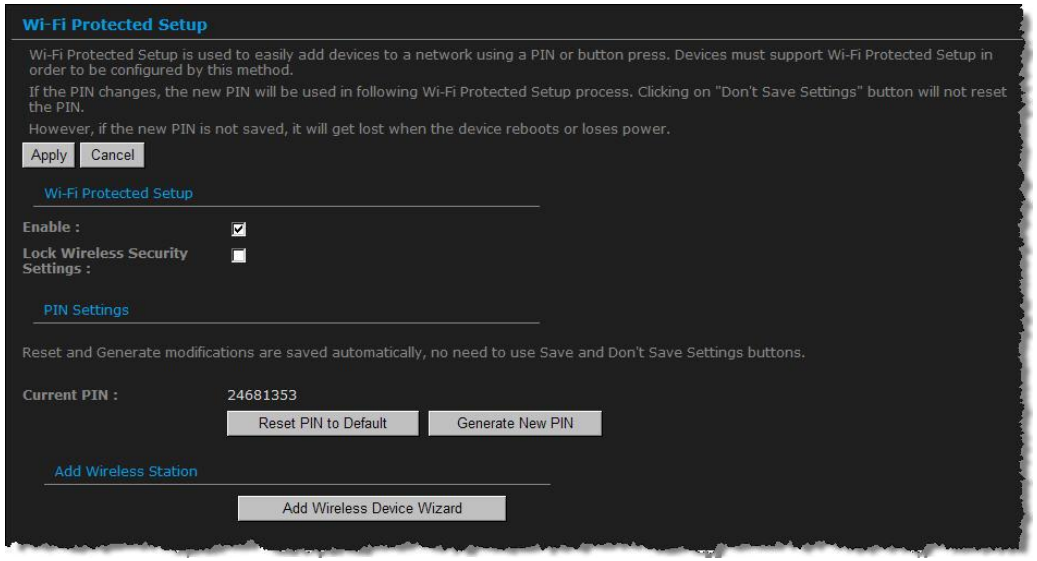


- **Enable WISH**: Place a check in this box to enable the WISH feature.

- **HTTP**: Place a check in this box to add HTTP as a classifier. This allows the device to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.
- **Windows Media Center**: Place a check in this box to add HTTP as a classifier. This enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.
- **Automatic**: Place a check in this box for the device to automatically configure the classifiers. When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.
- **Enable**: Place a check in this box to enable the WISH rule. A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required. WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.
- **Name**: Assign a meaningful name to the WISH rule.
- **Priority**: Select a priority from the drop-down list. The four priority message flows are:
- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).
- **Protocol**: Select a protocol from the drop-down list.
- **Hos1 IP Range**: Specify the IP range for the rule.
- **Host 1 Port Range**: Specify the port range for the rule.
- **Host 2 IP Range**: Specify the IP range for the rule.
- **Host 2 Port Range**: Specify the port range for the rule.
- Click on the **Save** button to insert the entry into the WISH rules list.

6.3.13. Wi-Fi Protected Setup

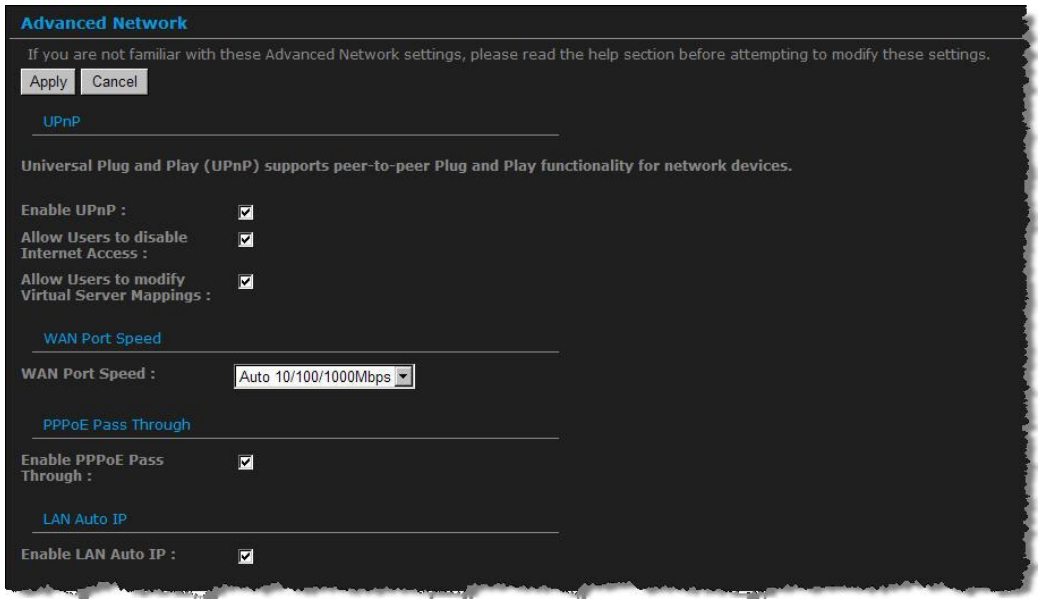
Wi-Fi Protected Setup is a feature that locks the wireless security settings and prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup.



- **Enable**: Place a check in this box to enable this feature.
- **Lock**: Place a check in this box to lock the wireless security settings and prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup.
- **Reset PIN to Default**: Press this button to reset the PIN to it's default setting.
- **Generate NEW PIN**: Press this button to generate a new random PIN.
- **Add Wireless Device Wizard**: Please refer to Chapter 4 in order to configure Wi-Fi Protected Setup using the Wizard.
- Click on the **Apply** button to store these settings.

6.3.14. Advanced Network (UPNP, WAN Ping…)

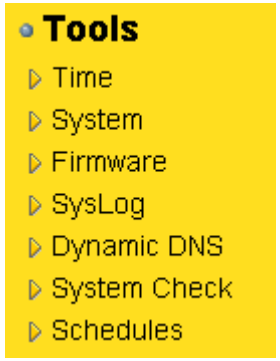
In this section you can configure the UPNP, WAN Ping, WAN port speed, multicast streams, and PPPoE pass-through settings.



- **Enable UPnP**: Place a check in this box to enable UPnP. UPnP stands for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This router has optional UPnP capability, and can work with other UPnP devices and software.
- **Allow Users to disable Internet Access**: Place a check in this box if you would like to allow to user to terminate the WAN session.
- **Allow Users to modify Virtual Server Mappings**: Place a check in this box if you would like the users to add, modify, or delete server mapping entries.
- **Enable WAN Ping Respond**: Place a check in this box if you would like this device to be pinged from the WAN side.
- **WAN Ping Inbound Filter**: You may select the computer that may ping this device from the WAN side.
- **WAN Port Speed**: You may select a WAN port speed from the drop-down list. It is recommended that you select **Auto**.

- **Enable Multicast Streams**: Place a check in this box to enable multicast streams. The router uses the IGMP protocol to support efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.
- **Enable PPPoE Pass Through**: Place a check in this box to enable PPPoE pass-through. This option controls whether LAN computers can act as PPPoE clients and negotiate the PPP sessions through the router over the WAN ethernet link. Enabling this option allows LAN computers to act as PPPoE clients. Disabling this option prevents LAN computers from establishing PPPoE pass-through connections.
- Click on the **Apply** button to store these settings.

6.4. Tools

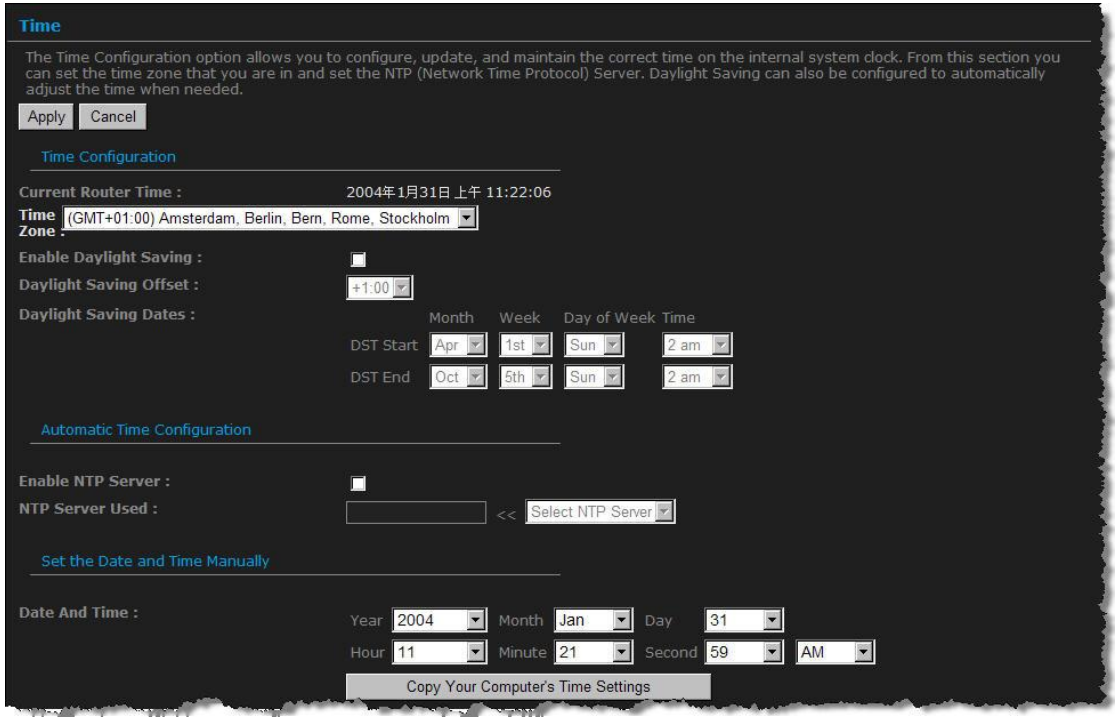


Click on the **Tools** link on the navigation drop-down menu. You will then see seven options: Time, System, Firmware, SysLog, Dynamic DNS, System Check, and Schedules. The configuration steps for each option are described below.

6.4.1.Time Zone Setting

Click on the **Time** link in the navigation menu. This feature allows you to configure, update, and maintain the correct time on the device's internal system clock as well as configure the time zone. The date and time of the device can be configured manually or by synchronizing with a time server.

Note: If the device losses power for any reason, it will not be able to keep its time running, and will not display the correct time once the device has been restarted. Therefore, you must re-enter the correct date and time.

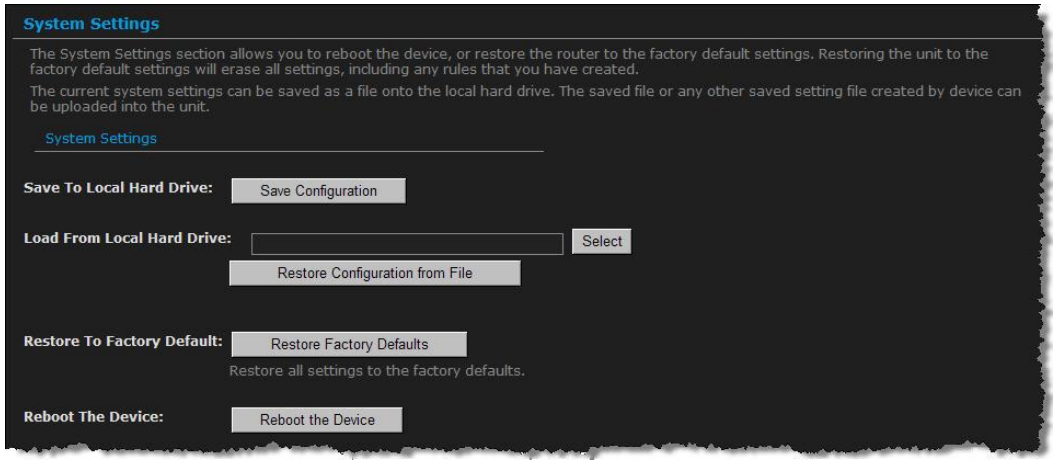


- **Current Router Time**: Displays the current time on the device.
- **Time Zone**: Select your time zone from the drop-down list.

- **Enable Daylight Saving**: Place a check in this box to enable daylight savings time.
- **Daylight Saving Offset**: Select the offset from the drop-down list.
- **Daylight Saving Date**: Select the daylight savings date from the drop-down list. Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun" and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM."
- **Enable NTP Server**: Place a check in this box if you would like to synchronize the device's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.
- **NTP Server Used**: Specify the NTP server or select one from the drop-down list.
- **Set the Date and Time**: Select a date and time from the drop-down list or do to use computer's time and date click on the **Copy Your Computer's Time Settings** button.
- Click on the **Apply** button once you have modified the settings.

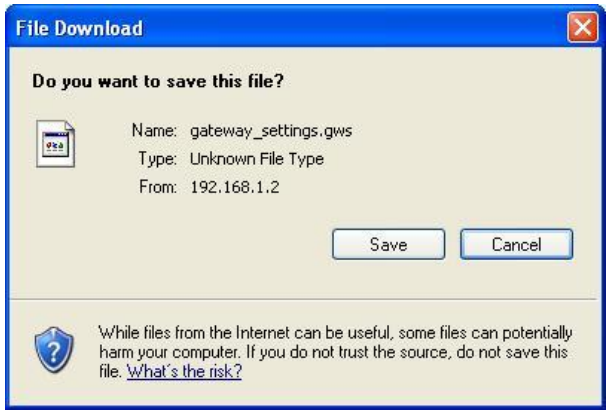
6.4.2.System

Click on the **System** link in the navigation menu. This page allows you to reboot the device using the current settings or restore all the settings to the factory defaults.



6.4.2.1. Save To Local Hard Drive

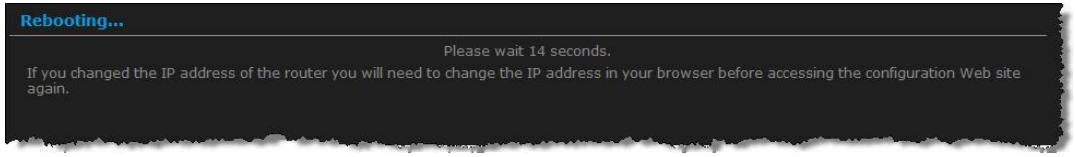
This option allows you to save the current configuration of the device into a file. Click on the **Save Configuration** button to begin.
Save the file on your local disk by using the **Save** or **Save to Disk** button in the dialog box.



6.4.2.2. Load From Local Hard Drive

This option allows you to restore a backup configuration from a file to the device. Click on the **Browse** button to select the file and then click on **Restore Configuration from a File** button.
The system then prompts you to reboot the device.

- Click on the **OK** button to continue. You will then see the **Rebooting** page.



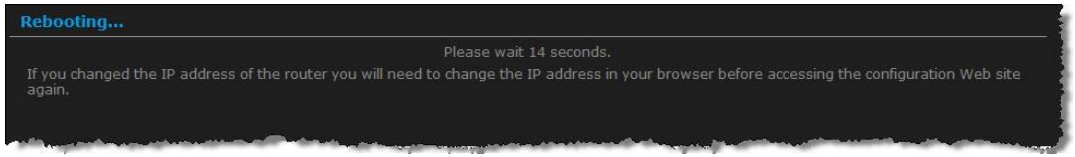
Please wait while the system is rebooting.
Note: Do no un-plug the device during this process as this may cause permanent damage.

6.4.2.3. Restore To Factory Default

Click on the **Restore all Settings to Factory Defaults** button. This option restores all configuration settings back to the settings that were in effect at the time when the device was shipped from the factory.

Once the dialog box appears, click on the **OK** button to confirm the action.
Note: The current settings will be lost.

- Click on the **OK** button to continue. You will then see the **Rebooting** page.



Please wait while the system is rebooting.
Note: Do no un-plug the device during this process as this may cause permanent damage.

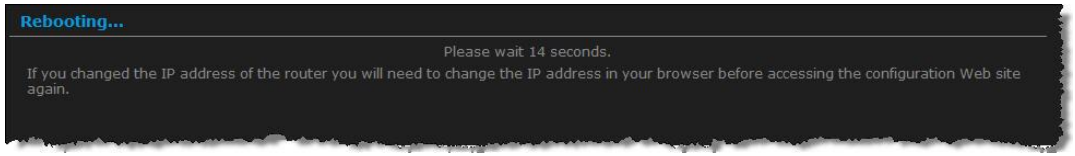
6.4.2.4. Reboot the device

- Click on the **Reboot the Device** button to reboot the device using its current settings. Once the dialog box appears, click on the **OK** button to confirm the action.

- Once the dialog box appears, click on the **OK** button to confirm the action.

Note: The current settings will be lost.

- Click on the **OK** button to continue. You will then see the **Rebooting** page.

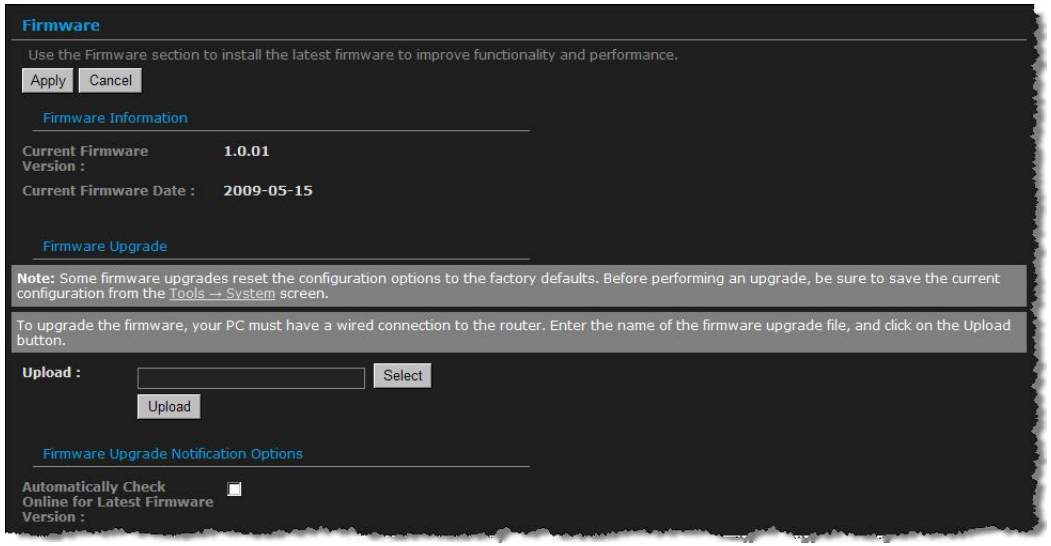


Please wait while the system is rebooting.

Note: Do no un-plug the device during this process as this may cause permanent damage.

6.4.3.Firmware Upgrade

- Click on the **Firmware** link in the navigation menu. This page allows you to upgrade the firmware of the device in order to improve the functionality and performance. This page also displays the current firmware version and its release date.

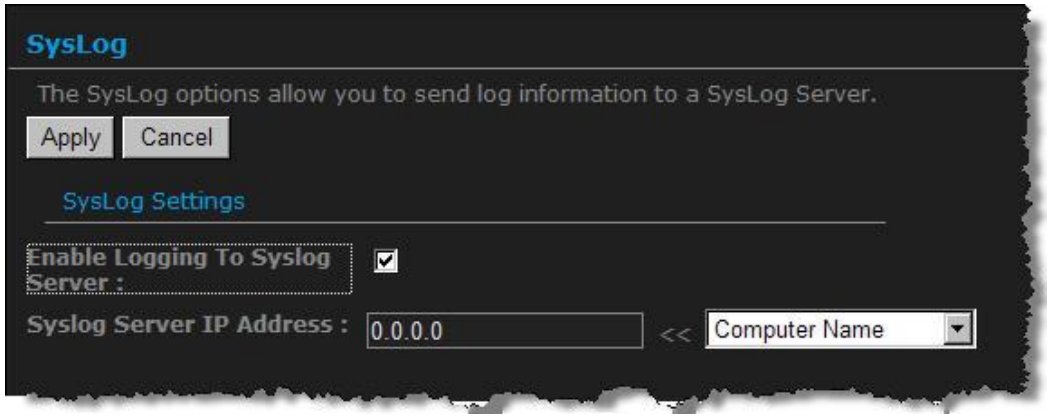


Ensure that you have downloaded the appropriate firmware from the vendor's website. Connect the device to your PC using an Ethernet cable, as the firmware cannot be upgraded using the wireless interface.

- Click on the **Browse** button to select the firmware and then click on the **Upload** button.

6.4.4.System Logs

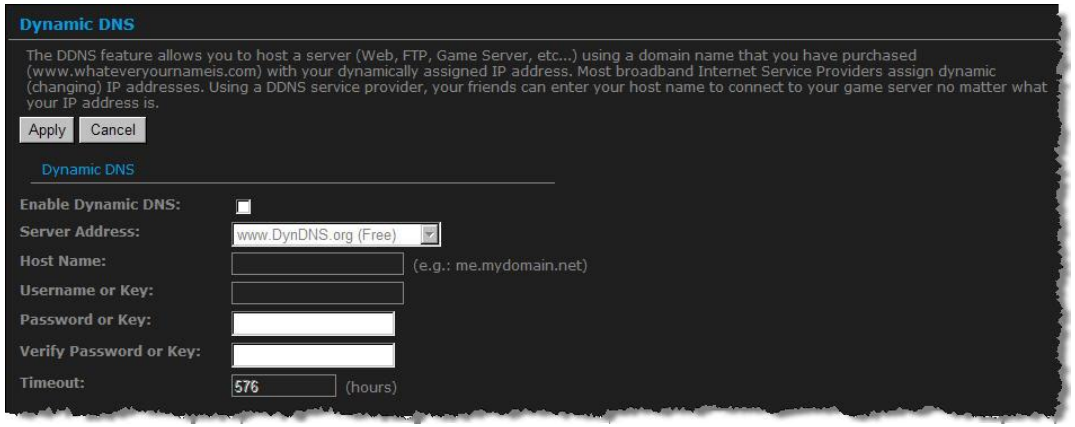
Logs display a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes



- **Enable Logging to a Syslog Server:** Place a check in this box to enable syslog logging.
- **Syslog Server IP Address:** Specify the IP address of the syslog server.
- Click on the **Apply** button once you have modified the settings.

6.4.5.Dynamic DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your host name to connect to your server, no matter what your IP address is.

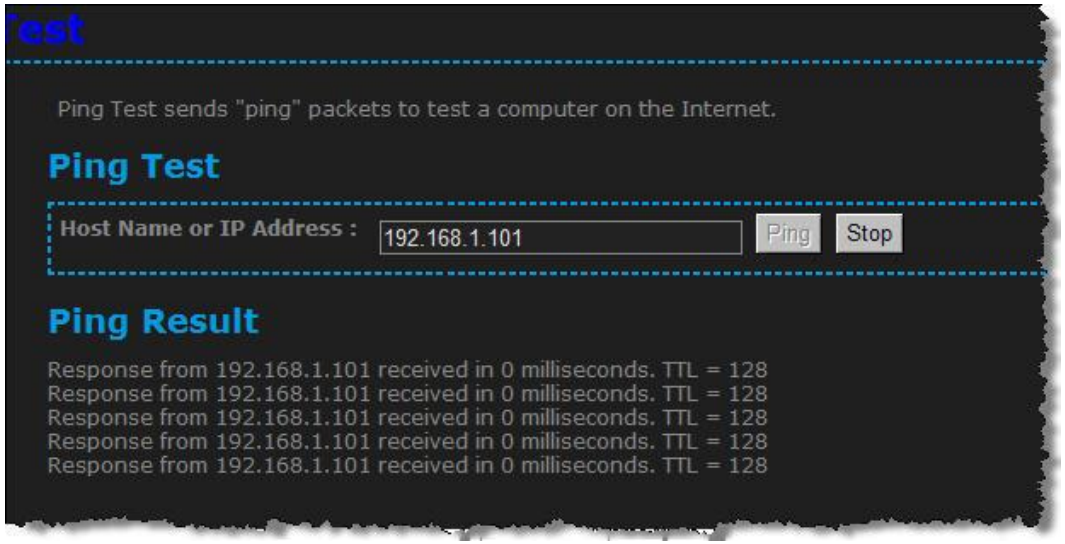


- **Enable Dynamic DNS**: Place a check in this box to enable the DDNS feature.
- **Service Address**: Select a DDNS service provider from the drop-down list. DynDNS is a free service while TZO offers a 30 day free trial.
- **Host Name**: Specify the website URL.
- **User Name**: Specify the user name for the DDNS service.
- **Password**: Specify the password for the DDNS service and verify it once again in the next field.
- **Timeout**: Specify the time between periodic updates to the Dynamic DNS, if the dynamic IP address has not changed. The timeout period is entered in hours.

Click on the **Apply** button once you have modified the settings.

6.4.6.System Check

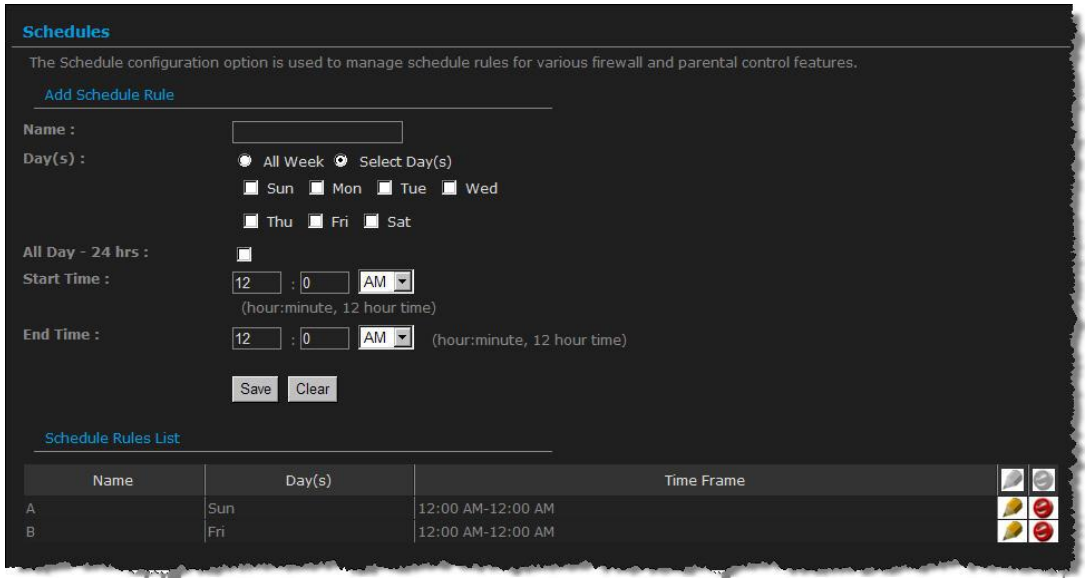
Click on the **System Check** link in the navigation menu. This page allows you to ping a host name or IP address.



Host Name or IP address: Specify the host name or IP address and then click on the **Ping** button.

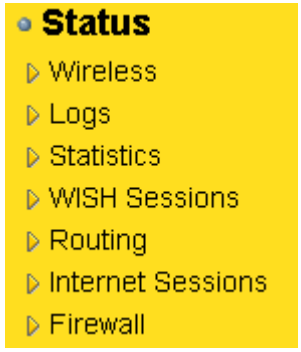
6.4.7.Schedules

Click on the **Schedules** link in the navigation menu. Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.



- **Name**: Specify a name for the schedule.
- **Day(s)**: Select the days at which you would like the schedule to be effective.
- **All Day – 24 hrs**: Place a check in this box if you would like the schedule to be active for 24 hours.
- **Start Time**: If you do not use the 24 hours option, you may specify a start time.
- **End Time**: If you do not use the 24 hours option, you may specify an end time.
- Click on the **Save** button to add this schedule into the list.

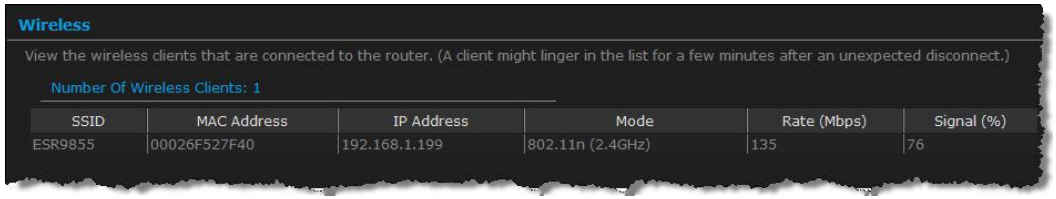
6.5. Status



Click on the **Status** link on the navigation tree menu. You will then see six options: Wireless, Logs, Statistics, WISH Sessions, Routing, and Internet Sessions. The configuration steps for each option are described below.

6.5.1. Wireless Status

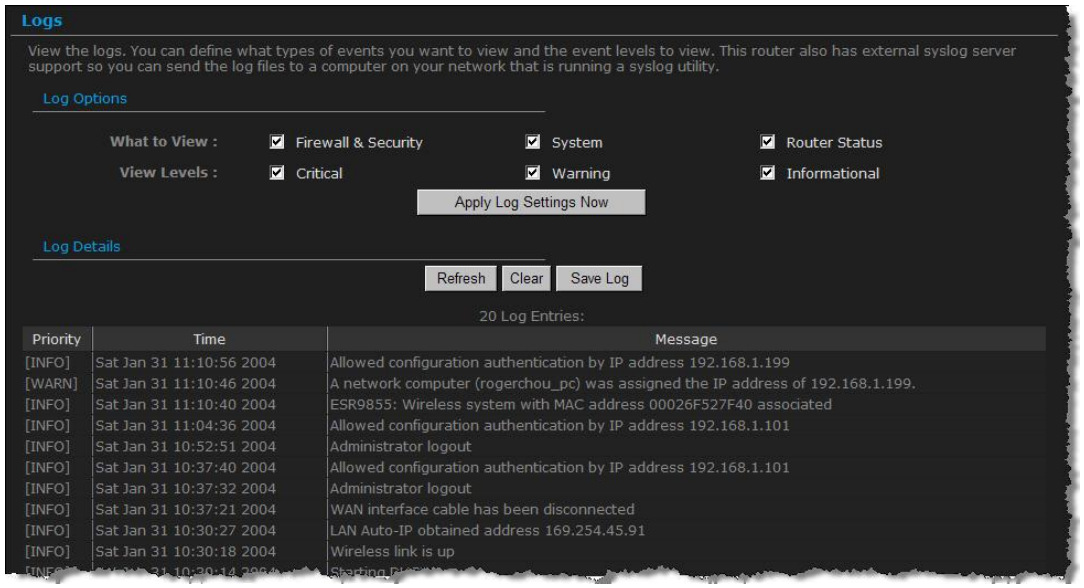
Click on the **Wireless** link in the navigation menu. The wireless section allows you to view the wireless clients that are connected to the device.



- **MAC Address**: The Ethernet ID (MAC address) of the wireless client.
- **IP Address**: The LAN-side IP address of the client.
- **Mode**: The transmission standard being used by the client. Values are 11a, 11b, 11g, or 11n for 802.11a, 802.11b, 802.11g, or 802.11n respectively.
- **Rate**: The actual transmission rate of the client in megabits per second.
- **Signal**: This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

6.5.2.Logs Status

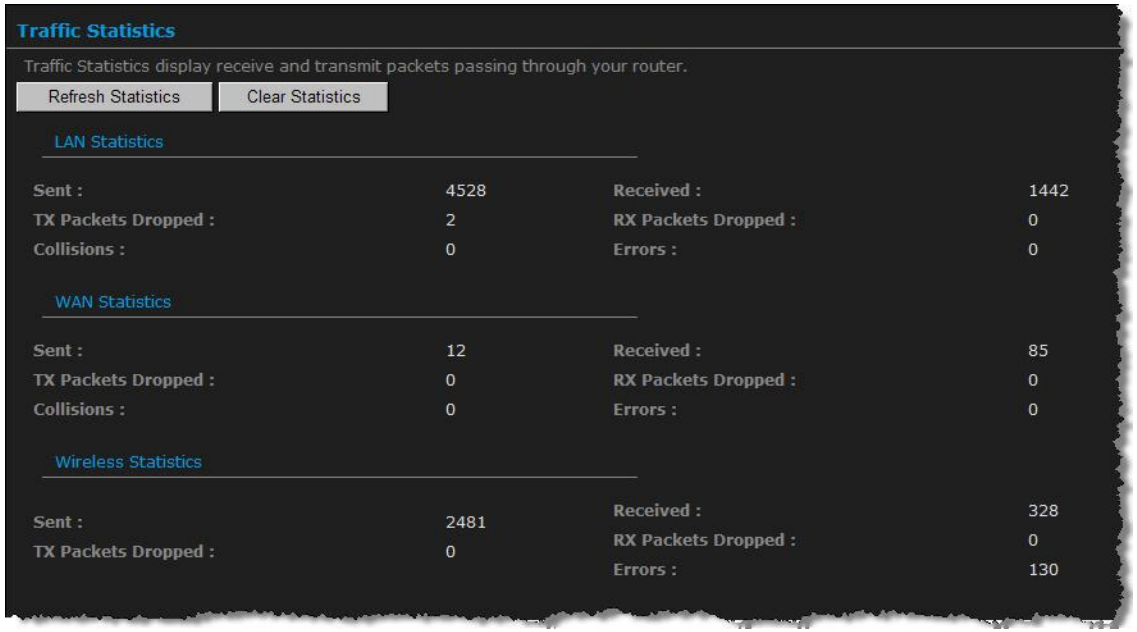
Click on the **Logs** link in the navigation menu. The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.



- **What to View**: Select the features of which you would like to view the logs: Firewall & Security, System, or Router Status.
- **View Levels**: Select the warning levels for the logs: Critical, Warning, or Informational.
- Click on the **Apply Log Settings Now** to make the new log effective.

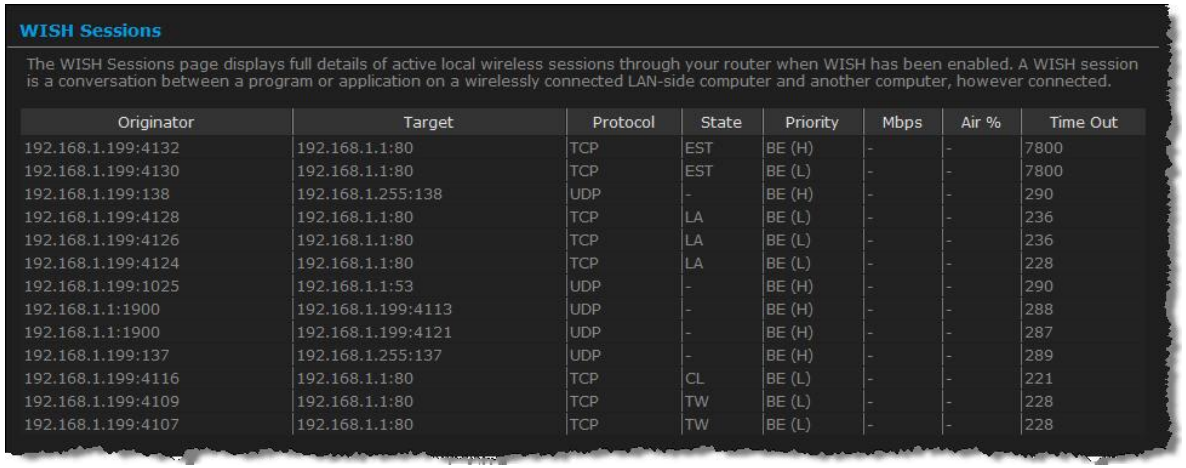
6.5.3.Statistics

Click on the **Statistics** link in the navigation drop-down menu. This page displays the transmitted and received packet statistics of the wired (LAN & WAN) and wireless interface. Click on the Refresh button to refresh the statistics.



6.5.4.WISH Session Status

Click on the **WISH Sessions** link in the navigation drop-down menu. The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.



WISH Sessions

The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

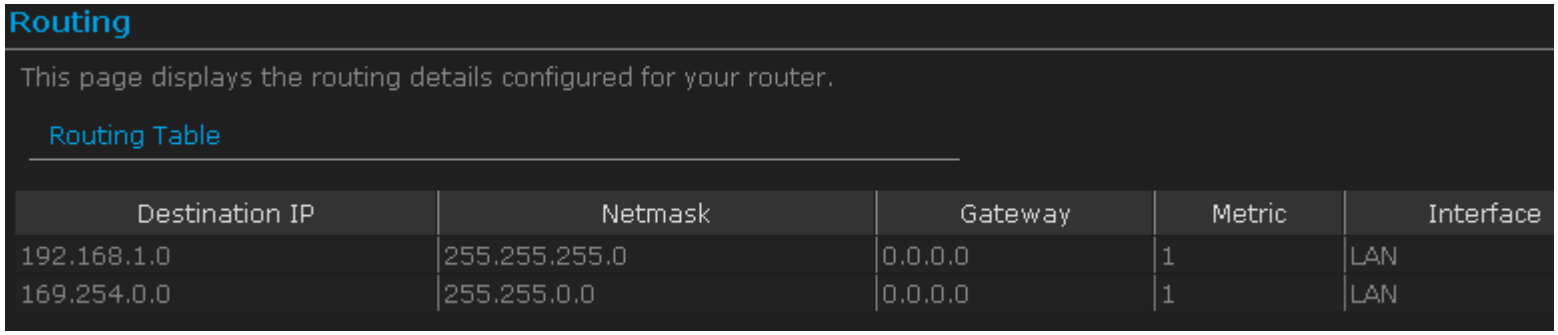
Originator	Target	Protocol	State	Priority	Mbps	Air %	Time Out
192.168.1.199:4132	192.168.1.1:80	TCP	EST	BE (H)	-	-	7800
192.168.1.199:4130	192.168.1.1:80	TCP	EST	BE (L)	-	-	7800
192.168.1.199:138	192.168.1.255:138	UDP	-	BE (H)	-	-	290
192.168.1.199:4128	192.168.1.1:80	TCP	LA	BE (L)	-	-	236
192.168.1.199:4126	192.168.1.1:80	TCP	LA	BE (L)	-	-	236
192.168.1.199:4124	192.168.1.1:80	TCP	LA	BE (L)	-	-	228
192.168.1.199:1025	192.168.1.1:53	UDP	-	BE (H)	-	-	290
192.168.1.1:1900	192.168.1.199:4113	UDP	-	BE (H)	-	-	288
192.168.1.1:1900	192.168.1.199:4121	UDP	-	BE (H)	-	-	287
192.168.1.199:137	192.168.1.255:137	UDP	-	BE (H)	-	-	289
192.168.1.199:4116	192.168.1.1:80	TCP	CL	BE (L)	-	-	221
192.168.1.199:4109	192.168.1.1:80	TCP	TW	BE (L)	-	-	228
192.168.1.199:4107	192.168.1.1:80	TCP	TW	BE (L)	-	-	228

- **Originator**: The IP address and, where appropriate, port number of the computer that originated a network connection.
- **Target**: The IP address and, where appropriate, port number of the computer to which a network connection has been made.
- **Protocol**: The communications protocol used for the conversation.
- **State**: State for sessions that use the TCP protocol.
- **NO**: None -- This entry is used as a placeholder for a future connection that may occur.
- **SS**: SYN Sent -- One of the systems is attempting to start a connection.
- **EST**: Established -- the connection is passing data.
- **FW**: FIN Wait -- The client system has requested that the connection be stopped.
- **CW**: Close Wait -- the server system has requested that the connection be stopped.
- **TW**: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- **LA**: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.

- **CL**: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.
- **Priority**: The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:
- **BK**: Background (least urgent).
- **BE**: Best Effort.
- **VI**: Video.
- **VO**: Voice (most urgent).
- **Time Out**: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.
- **300 seconds** - UDP connections.
- **240 seconds** - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
- **7800 seconds** - Established or closing TCP connections.

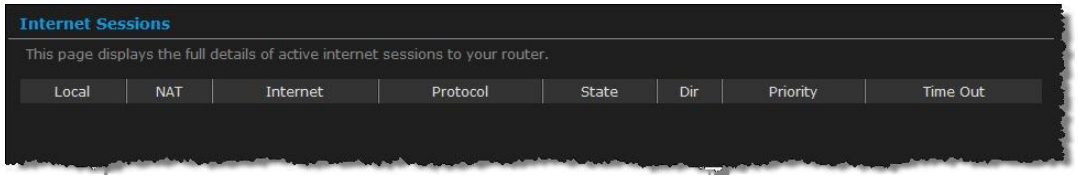
6.5.5.Routing

This function shows current routing table



6.5.6.Internet Session Status

Click on the **Internet Sessions** link in the navigation drop-down menu. The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

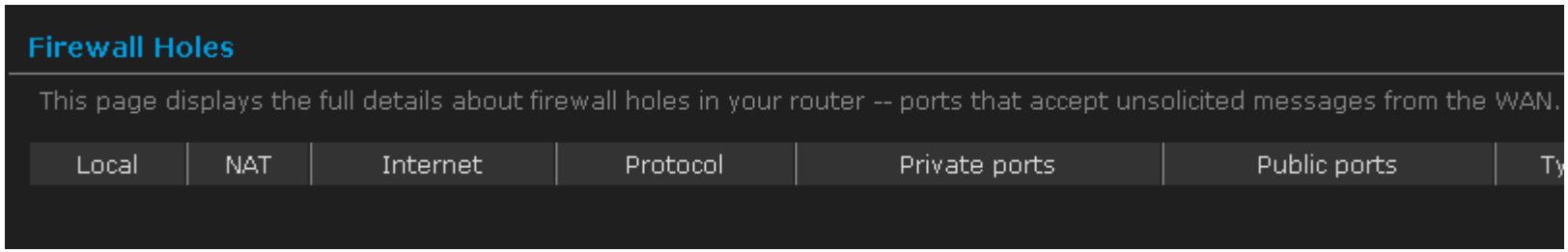


- **Local**: The IP address and, where appropriate, port number of the local application.
- **NAT**: The port number of the LAN-side application as viewed by the WAN-side application.
- **Internet**: The IP address and, where appropriate, port number of the application on the Internet.
- **Protocol**: The communications protocol used for the conversation.
- **State**: State for sessions that use the TCP protocol.
- **NO**: None -- This entry is used as a placeholder for a future connection that may occur.
- **SS**: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- **FW**: FIN Wait -- The client system has requested that the connection be stopped.
- **CW**: Close Wait -- the server system has requested that the connection be stopped.
- **TW**: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- **LA**: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- **CL**: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.
- **Priority**: The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are:
- **BK**: Background (least urgent).
- **BE**: Best Effort.
- **VI**: Video.
- **VO**: Voice (most urgent).
- **Time Out**: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

- **300 seconds** - UDP connections.
- **240 seconds** - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.
- **7800 seconds** - Established or closing TCP connections.

6.5.7.Firewall

This page displays the full details about firewall holes in your router -- ports that accept unsolicited messages from the WAN.



Appendix A – Glossary

8

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Ad-hoc network

Peer-to-Peer network between wireless clients

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C

Cable modem

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

DB-25

A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the sane time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

H.323

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J

Java

A programming language used to create programs and applets for web pages

K

Kbps

Kilobits per second

Kbyte

Kilobyte

L

L2TP

Layer 2 Tunneling Protocol

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

M

MAC Address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V

Virtual Private Network

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W

Wake on LAN

Allows you to power up a computer though it's Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

Appendix C – FCC Interference Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.